UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, v. JASON GALANIS, GARY HIRST, JOHN GALANIS, a/k/a "Yanni," HUGH DUNKERLEY, MICHELLE MORTON, DEVON ARCHER, and BEVAN COONEY, Defendants.	No. 16 Cr. 371 (RA)

DEVON ARCHER'S CORRECTED† MEMORANDUM OF LAW IN SUPPORT OF HIS MOTION TO SUPPRESS THE FRUITS OF TWO POST-INDICTMENT STORED COMMUNICATIONS ACT WARRANTS

Matthew L. Schwartz
BOIES SCHILLER FLEXNER LLP
575 Lexington Avenue, 7th Floor
New York, New York 10022
Tel.: (212) 446-2300
Fax: (212) 446-2350
mlschwartz@bsfllp.com

Attorneys for Devon Archer

† This corrected memorandum of law fixes certain citation forms, typos, and other non-substantive errors. It is otherwise materially identical to the originally-filed version.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

PRELIMINARY STATEMENT

In December 2016, seven months after filing its initial charges in this case, the government finally realized that it had failed to properly investigate Mr. Archer's purported role in the crimes charged in the Indictment. Based on a small handful of e-mails that Mr. Archer had received (not sent) more than two years earlier, the government obtained warrants to search four internet service provider accounts associated with Mr. Archer and his assistant, as well as one account associated with a co-defendant. From the moment that Mr. Archer learned about the warrants, he has pointed out to the government and the Court that they are deeply defective for a variety of reasons.

First of all, the warrants are facially unconstitutional because they authorize a search for "evidence of crime" untethered to any specific facts or criminal offenses. The Supreme Court has long recognized that such "general warrants" are overbroad and impermissible.

Second, the affidavit underlying the warrants utterly fails to provide the necessary probable cause. The evidence cited in the affidavit is hopelessly stale, and with respect to Mr. Archer and his assistant's Google accounts, is based on a single e-mail from more than two years before the warrants were issued. The warrants also authorize the government to search through and seize two dozen discrete categories of information stored in a variety of different places – ranging from e-mails to photographs to browser histories to the contents of cloud storage drives – when the affidavit is entirely silent on everything but e-mails.

Moreover, although the warrant affidavit is defective standing alone, it also omits critical information that, had it been included, would have surely caused the Magistrate Judge to refuse to issue the warrants. Among other things, the affidavit intentionally or recklessly failed to disclose that Mr. Archer had previously produced to the government thousands of e-mails from the two of his accounts targeted by the warrants. Had the magistrate known this – and known

that the government was still only able to come up with a few ambiguous-at-best e-mails – it would have been all the more obvious just how stale the evidence cited in the affidavit was and how unlikely it was that any other evidence would be recovered.

Finally, the government also executed the warrant in an unconstitutional fashion. It not only invaded Mr. Archer's legal privilege, but it also seized (and produced to all defense counsel in this case) tens of thousands of intensely personal and concededly irrelevant and non-responsive communications. This Court has in fact already found that the government "produced all of the materials obtained pursuant to the warrant . . . without regard to responsiveness. Many of these documents have no relevance to the facts of this case and are personal and/or confidential in nature." *See* Declaration of Matthew L. Schwartz ("Decl.") Ex. 24 at 4. Even if the Court finds that the warrants were not unconstitutional "general warrants" on their faces, by so blatantly ignoring the warrants' scope, the government, in effect, conducted an unconstitutional general search, the fruits of which must be suppressed.

Mr. Archer repeatedly raised these concerns prior to the government's execution of the warrants, when the problems with the warrants could still have been cured, but the government insisted on going forward, acknowledging that "the risk is on the government." The government must now bear the consequences of taking that risk, and the Court should suppress all evidence derived directly or indirectly from the warrants.

RELEVANT BACKGROUND[1]

A. The Investigation

Beginning in at least 2015, the United States Attorney's Office for the Southern District of New York and the U.S. Securities and Exchange Commission commenced investigations into

[1] This section sets out facts generally relevant to Mr. Archer's suppression motion. Additional facts that may be specific to particular arguments are set out below.

a series of bonds (the "Bonds") offered by the Wakpamni Lake Community Corporation (the "WLCC"). As part of their coordinated investigations, both the U.S. Attorney's Office and the SEC issued subpoenas directed to Mr. Archer, the scope of which the U.S. Attorney's Office directed Mr. Archer's counsel to negotiate with the SEC, which resulted in an agreed-upon date range and list of search terms for Mr. Archer's production. *See* Decl. ¶¶ 37-38. Beginning in May 2016, Mr. Archer produced over 7,600 documents comprising more than 61,000 pages of material to the SEC and the U.S. Attorney's Office. *Id.* ¶ 38.

During the course of the investigation, Mr. Archer's counsel also met simultaneously with representatives of the U.S. Attorney's Office and the SEC on two occasions. *Id.* ¶ 40. At the second meeting – which took place on a Friday, and which occurred while Mr. Archer was still in the process of making a rolling production of documents responsive to the subpoenas – representatives of the U.S. Attorney's Office informed Mr. Archer's counsel that Mr. Archer needed to produce any documents that he wished for the government to consider by the immediately following Monday. *Id.* Notwithstanding this unreasonably short three-day deadline, Mr. Archer's counsel worked diligently over the weekend and made a substantial production of documents to the government the following Monday, including nearly 3,500 documents from the e-mail accounts darcher@rosemontseneca.com and darcher@rosemontcapital.com. *Id.* ¶ 38. Unbeknownst to Mr. Archer or his lawyers, however, the government had already obtained a sealed criminal complaint earlier that same day [ECF No. 1].

B. The Indictment[2]

On May 31, 2016, a Grand Jury in this District returned a four-count indictment charging seven defendants in four counts [ECF No. 22]. Mr. Archer, the sixth named defendant, was charged solely in Counts One and Two, which allege conspiracy to commit securities fraud and substantive securities fraud. He was not charged in Counts Three and Four, which allege conspiracy to commit investment adviser fraud and substantive investment adviser fraud. On November 2, 2016, the Grand Jury returned a superseding indictment charging the same seven defendants in the same four counts; the only material difference was the addition of certain "speaking" allegations [ECF No. 90].

C. The Post-Indictment Warrants

On or about December 28, 2016 – long after it had charged Mr. Archer – the government sought and obtained from the Honorable Barbara Moses two warrants, both based on a single application and affidavit. The warrants, issued pursuant to the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A) (the "SCA") and Federal Rule of Criminal Procedure 41, called generally for documents associated with five separate internet service provider accounts.

Two of those accounts were associated with Mr. Archer: darcher@rosemontseneca.com, which was a Google account (the "Archer Google Account," referred to in the warrant application as the "Archer Seneca Account"), and darcher@rosemontcapital.com, which was an Apptix account (the "Archer Apptix Account," referred to in the warrant application as the "Archer Account"; in this memorandum, these two accounts are together referred to as the

[2] In this memorandum, references and citations to the "Indictment" are to the first superseding indictment, returned on or about November 2, 2016 [ECF No. 90], unless otherwise specified.

"Archer Accounts"). Two of the other accounts were associated with Mr. Archer's assistant, Sebastian Momtazi, who is not a defendant in this case: smomtazi@rosemontseneca.com, a Google account (the "Momtazi Google Account," referred to in the warrant application as the "Momtazi Seneca Account"), and smomtazi@rosemontcapital.com, an Apptix account (the "Momtazi Apptix Account," referred to in the warrant application as the "Momtazi Account"; in this memorandum, these two accounts are together referred to as the "Momtazi Accounts"). The fifth and final account belonged to co-defendant Bevan Cooney: btcooney@gmail.com, a Google account (referred to herein and in the warrant application as the "Cooney Account"; in this memorandum, the Archer Accounts, the Momtazi Accounts, and the Cooney Account are collectively referred to as the "Targeted Accounts").

One of the two warrants targeted Messrs. Archer, Momtazi, and Cooney's Google accounts (the "Google Warrant"). *See* Decl. Ex. 5 at 1-11. The other warrant targeted Messrs. Archer and Momtazi's Apptix accounts (the "Apptix Warrant" and, together with the Google Warrant, the "Warrants"). *See id.* at 12-17.

1. The Warrant Application And Supporting Affidavit

Both of the Warrants, covering all five Targeted Accounts, were issued on the basis of a single December 28, 2016 affidavit from FBI Special Agent Shannon Bieniek, which also attached and incorporated the Indictment (the "Bieniek Affidavit"). *See* Decl. Ex. 4.[3] The Bieniek Affidavit stated that the government was making "an application for search warrants pursuant to [the SCA] for all content, including emails and draft emails, created, sent or received

[3] Both the Bieniek Affidavit itself and the attached Indictment contain numbered paragraphs starting from one. So as to avoid confusion, this memorandum refers to page numbers, with the first twenty pages comprising Special Agent Bieniek's affidavit and the next twenty-four pages comprising the attached Indictment.

between January 1, 2014 and May 11, 2016, inclusive, and other information associated with" the Targeted Accounts. *Id.* at 1-2.

The Bieniek Affidavit asserted that there was probable cause to believe that the Targeted Accounts contained "evidence, fruits, and instrumentalities" of all four crimes charged in the Indictment – *i.e.*, securities fraud, conspiracy to commit securities fraud, investment adviser fraud, and conspiracy to commit investment adviser fraud – which the Bieniek Affidavit defined as the "Subject Offenses," *see id.* at 2. Based on her review of "business records, bank records, telephone records, public records, email correspondence, [and] court filings," and her conversations with "SEC staff attorneys about their review of such records," Special Agent Bieniek "concluded that there [was] probable cause to believe that Devon Archer and Bevan Cooney ha[d] engaged in the Subject Offenses," *id.* at 9, notwithstanding the fact that neither Mr. Archer nor Mr. Cooney had been charged in the investment adviser fraud counts. *Compare id.* at 2, 9 *with id.* at 39-42 (section of Indictment charging only Jason Galanis, Gary Hirst, and Michelle Morton with investment adviser fraud and conspiracy to commit investment adviser fraud).

The Bieniek Affidavit began by summarizing the government's investigation, which it said had begun in "at least 2015." *Id.* at 9. Notably, and as discussed further at Point II below, the Bieniek Affidavit failed to disclose either that Mr. Archer had previously produced nearly 3,500 documents to the government from the Archer Accounts, or – aside from a passing reference to speaking with SEC staff attorneys, *see id.* – that the SEC had conducted its own substantial coordinated investigation, including putting the investment advisory firms at issue in this case into receivership and obtaining all of their records.

The Bieniek Affidavit then summarized the Indictment, *see id.* at 9-11, and set out the purported probable cause for the issuance of the Warrants.

The Bieniek Affidavit asserted generally that the Targeted Accounts were involved in e-mail correspondence concerning "the initiation of the scheme to orchestrate the issuance of" the Bonds, the placement of the Bonds with clients of captive investment advisory firms, and the use of the proceeds of the Bonds. *Id.* at 12. More specifically, the Bieniek Affidavit set forth a handful of specific examples of communications involving the Targeted Accounts, all of which were sent between April and October 2014.

Parsed by account, the Bieniek Affidavit set out the following bases to assert that there was probable cause with respect to each of the Archer Accounts and Momtazi Accounts. Notably, with only one exception, Mr. Archer was merely a recipient of or carbon copy on, rather than the sender of, each of the communications that purportedly supplied probable cause.

a. The Purported Probable Cause To Search The Archer And Momtazi Google Accounts

The Bieniek Affidavit contains precisely one and only one paragraph purporting to supply probable cause to search the Archer Google Account and the Momtazi Google Account:

> Also in furtherance of the scheme, by letter dated October 1, 2014, Archer provided false and misleading information to the Independent Trustee of an asset manager affiliated with the placement agent for the Tribal Bonds, which had sought assurances from Archer that Jason Galanis would not be involved with either the placement agent or related entities. On or about September 26, 2014, Momtazi sent a copy of the letter from the MOMTAZI SENECA ACCOUNT to an employee of the placement agent, cc'ing the ARCHER SENECA ACCOUNT.

Id. at 16. This paragraph would seem to reference the same conduct alleged in Paragraph 10 of the Indictment – that Mr. Archer, "who was affiliated with the Placement Agent, falsely represented to affiliates of the Placement Agent that, among other things, JASON GALANIS would not be involved with any entities affiliated with the Placement Agent or source deals to the Placement Agent." Neither the Bieniek Affidavit nor the Indictment explain how this alleged

misstatement to "an asset manager affiliated with the placement agent" had anything to do with the offenses charged in the Indictment, particularly because the Indictment specifically alleges that the "placement agent" did not, in fact, place any of the Bonds. *Id.* at 26 (Indictment ¶ 9).

b. The Purported Probable Cause To Search The Archer Apptix Account

With respect to the Archer Apptix Account, the Bieniek Affidavit recounts four kinds of conversations:

- Three e-mails sent by Jason Galanis to the Archer Apptix Account and the Cooney Account that allegedly kept Messrs. Archer and Cooney "apprised" of the status of the WLCC bond issuance, and one reply e-mail from the Cooney Account. *Id.* at 12-13. These e-mails were dated April 4, July 5, and August 14, 2014, and were allegedly sent by Jason Galanis or Cooney, not by Mr. Archer, and Mr. Archer is not alleged to have responded to any of them. *See id.*

- Two e-mails sent by Jason Galanis to the Archer Apptix Account and the Cooney Account that allegedly kept Messrs. Archer and Cooney "apprised" of his "efforts to gain control of" an investment advisory firm. These e-mails were dated May 9 and July 16, 2014. *Id.* at 14-15. This is the one place in the entire Bieniek Affidavit where Mr. Archer allegedly responded to an e-mail. According to the Bieniek Affidavit, Jason Galanis updated Messrs. Archer and Cooney about a term sheet to acquire one of the investment advisory firms, and further wrote: "Firm manages $900 million on a discretionary basis for 28 institutional clients (pensions and endowments). . . . We have agreed to give the firm an opportunity to participate in the native American bond new issues. I believe they will take $28 million of the Wakpamni/Ogala [sic] Sioux issue that Greenberg Traurig is working on." *Id.*at 14. Allegedly, Mr. Archer responded by writing, from the Archer Apptix Account, "This is very encouraging!" *Id.*

- Three e-mails sent by Mr. Momtazi from the Momtazi Apptix Account to a brokerage firm about the potential purchase of some of the Bonds, which cc'd the Archer Apptix Account. *Id.* at 15-16. These e-mails were dated September 29, October 1, and October 24, 2014, and were all allegedly sent by Mr. Momtazi. *See id.* Mr. Archer is not alleged to have responded to any of these e-mails.

- One e-mail sent by Jason Galanis to the Archer Apptix Account and the Cooney Account, allegedly regarding Jason Galanis's plans for an initial public offering of a company not mentioned in the Indictment. *Id.* at 16-17. This e-mail was dated February 25, 2014, and Mr. Archer is not alleged to have responded to it. *See id.*

c. The Purported Probable Cause To Search The Momtazi Apptix Account

The sole purported basis for probable cause to search the Momtazi Apptix Account was Mr. Momtazi's three e-mails to a brokerage firm about the potential acquisition of some of the Bonds, as referenced in the third bullet-point above. *Id.* at 15-16.

d. The Information Sought By The Government

On the basis of this purported showing of probable cause, the Bieniek Affidavit listed the following nineteen categories of documents, information, and data maintained by Google and (in some cases) Apptix with respect to the Targeted Accounts,[4] all of which it sought permission to search:

- Email contents;
- Google Docs, Sheets, and Slides;
- Google Drive content;
- Google Chats and Hangouts content;
- Address book;
- Subscriber and billing information;
- Transactional information;
- Customer correspondence;
- Location data;
- Picasa Web Albums;
- Android Services;
- Web History;
- Google Alerts;
- Google Webmaster Tools and Google Search Console;
- Google Analytics;
- Google Payments;
- Google Apps and Google Apps Administrator Control Panel;
- Google URL Shortener; and
- Preserved and backup records.

Id. at 3-8 & n.1. Several of these categories are obviously compound – *e.g.*, the categories seeking "Google Docs, Google Sheets, and Google Slides" content or "Google Chats and Google

[4] Some of these categories, most notably the ones that specifically reference Google, were relevant only to the three Google Accounts.

Hangouts content." *See id.* at 3-4, 6-8. Thus, in actuality, the Bieniek Affidavit sought permission to search and seize twenty-four discrete categories of documents, information, and data, twenty-three of which went beyond "[e]mail contents." *Id.* at 3.

The Bieniek Affidavit stated that the requested warrants would be transmitted to Google and Apptix, which would "be directed to produce a digital copy of any responsive records to law enforcement personnel within 30 days from the date of service." *Id.* at 19. It further stated that "law enforcement officers and agents," as well as perhaps "attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control," would "retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses." *Id.* The Bieniek Affidavit then stated that "law enforcement personnel might use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails," "keyword searches," and "other methods as well." *Id.*

2. The Warrants Themselves

On the basis of the Bieniek Affidavit, Magistrate Judge Moses signed both of the Warrants. *See id.* at 45, 56. The Warrants directed Google and Apptix to provide to the FBI the records listed in "Attachment A" "for subsequent review by law enforcement personnel." *Id.*

a. The Scope Of Places To Be Searched

Attachment A to each of the Warrants directed Google and Apptix to produce an electronic copy of certain enumerated categories of documents, information, and data contained in or associated with the Targeted Accounts from the period from January 1, 2014 through May 11, 2016, to the extent such materials were within Google and Apptix's "possession, custody, or control." *See id.* at 47, 58. Attachment A to the Google Warrant replicated the full list of twenty-four categories of documents, information, and data set forth in the Bieniek

Affidavit, *see id.* at 47-53, while Attachment A to the Apptix Warrant listed six categories of information maintained by Apptix: "Email contents, "Address book," "Subscriber and billing information," "Transactional information," "Customer correspondence," and "Preserved records," *id.* at 58-59.

b. The Scope Of Things To Be Seized

Attachment A to each of the Warrants also echoed the Bieniek Affidavit in stating that "law enforcement officers and agents," as well as perhaps "attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control," were authorized to review the records produced by Google and Apptix. *Id.* at 53, 60.

Unlike the Bieniek Affidavit, which purported to supply probable cause to seize evidence related to the four Subject Offenses, the Warrants themselves authorized the government to effect a far broader seizure, including:

> evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1348, and Title 15, United States Code, Sections 78j(b) and 78ff, Title 17, Code of Federal Regulations, Sections 240.10b-5; conspiracy to commit securities fraud, in violation of Title 18, United States Code, Section 371; investment advisor fraud, in violation of Title 15, United States Code, Sections 80b-6 and 80b-17; and conspiracy to commit investment adviser fraud, in violation of Title 18, United States Code, Section 371, *among other statutes*, including the following:
>
> * * *
>
> - *evidence of crime* (*e.g.*, agreement to engage in unlawful conduct, references to or discussion of unlawful conduct), *communications constituting crime* (*e.g.*, emails containing fraudulent representations) . . . .

Id. at 53, 60 (emphases supplied).

D. The Pre-Execution Litigation

Notwithstanding the fact that the Warrants were never sealed, the government failed to produce them or the Bieniek Affidavit in discovery.[5] As a result, Mr. Archer was unaware of the existence of either of the Warrants until nearly a month after they were issued, when, on the evening of January 26, 2017, Google provided him with notice that it had received the Google Warrant and that, per company policy, it would produce responsive documents to the government unless Mr. Archer filed an objection or motion to quash. *See* Decl. Ex. 6. Google also provided a redacted version of the Google Warrant. *See id.*

The very next day, counsel for Mr. Archer contacted the government to request a copy of the unredacted Google Warrant and its supporting application, and to seek the government's consent to hold off on collecting responsive data until Mr. Archer's defense team had an opportunity to review the requested documents. *See* Decl. Ex. 7. The government advised counsel that it did not believe that the Google Warrant and its supporting application were "presently discoverable," and that it would only produce them later, along with the results of its search. *See id.* The government also informed Mr. Archer's counsel that it would not agree to instruct Google to hold off on producing responsive documents. *See id.* The government did not, however, mention the existence of the Apptix Warrant.

[5] The Bieniek Affidavit cites 18 U.S.C. § 2705(b) for the proposition that the government could have sought and obtained an order precluding Google and Apptix from notifying Mr. Archer of the existence of the Warrants if there was "reason to believe that such notification will seriously jeopardize an investigation." Decl. Ex. 4 at 9. Mr. Archer is not aware of the government having sought any such order in this instance, and the Bieniek Affidavit sets forth no facts on which anyone could conclude that notice would jeopardize any investigation, particularly in view of the fact that the government's investigation was not only overt at that point, but had already led to the publicly-filed Indictment.

1. In The District Court

Later that same day, Mr. Archer filed an emergency motion seeking an order (1) compelling the government to produce full, unredacted copies of the Google Warrant and its supporting application, and (2) enjoining Google from producing responsive data until Mr. Archer "had a reasonable amount of time to review the warrant and application and determine whether to challenge" the warrant. Decl. Ex. 7 at 1.

As to the government's failure to produce the Google Warrant and its supporting application, Mr. Archer argued that such material was plainly subject to discovery under Federal Rule of Criminal Procedure 16, and is routinely produced in discovery by the government in this district. *Id.* at 2.

As to his request that the government be enjoined from reviewing any of the fruits of the Google Warrant, Mr. Arched argued that he "should be permitted to examine the warrant and application, and make any appropriate challenges, *before* the government searches the data." *Id.* (emphasis in original). Mr. Archer contended that, "even based on the very limited information [then] available to the defense" given that it only had access to a redacted copy of the Google Warrant and no access to the Bieniek Affidavit at all, it nevertheless appeared "that the warrant [would] be subject to challenge on numerous grounds." *Id.* Among other things, Mr. Archer flagged the fact that "the face of the warrant reveals that it is almost surely overbroad, . . . amount[ing] to an unconstitutional general search," insofar as it called for not only e-mails from the Google Account, "but also all Google Docs documents, all contents of Google Drive, all photographs stored on Picasa Web Albums, all internet browsing activity, all location data, and other expansive categories of information." *Id.* Mr. Archer also argued that he "would be severely prejudiced by the government's review of . . . literally hundreds of attorney-client communications" contained in the Google Account, as the Google Warrant "appear[ed] to

contain absolutely no restriction on the government's ability to access attorney-client materials." *Id.*[6] Accordingly, Mr. Archer contended that, if there was a basis to challenge the Google Warrant, "the Court should hear it *before* the government gains access to this massive amount of data." *Id.* at 3 (emphasis supplied). Mr. Archer also pointed out that "[d]elaying a search of the data would cause no prejudice to the government" because "Google maintains a copy of data requested by the government while any legal process is challenged," such that there would be "no risk that data will be lost." *Id.* (citing Google Transparency Report).

The government responded to Mr. Archer's motion on January 30, 2017, disclosing for the first time that, in addition to the Google Warrant, it had also obtained the Apptix Warrant based on the same warrant application. *See* Decl. Ex. 8 at 1. The government also disclosed that it had already received a responsive production from Apptix, and that it was therefore "prepared to produce" the unredacted Warrants and the supporting application to all defense counsel, and would do so later that week, *id.* at 1-2, apparently on the theory that its Rule 16 obligation only arose after the execution of one of the two Warrants. In general, the government argued that any pre-execution challenge to the Warrants was premature, and that Mr. Archer would have a full opportunity to challenge the Warrants through a suppression motion. *See id.* at 2-4.

At a conference on January 31, 2017, after the government acknowledged that "the risk" stemming from the myriad problems with the Warrants was "on the government," Decl. Ex. 9

[6] While Mr. Archer's motion pointed out that the Google Warrant "contain[ed] no restrictions on the government's review of attorney-client materials, and no procedures for allowing the defense to conduct a privilege review, the use of a 'taint team' or 'wall AUSA,' or other minimization procedures," it also forcefully argued that the use of a "taint team" or "wall AUSA" would not be acceptable in this case, citing numerous courts that have described why such procedures are inappropriate in criminal cases. Decl. Ex. 7 at 3-4.

at 16:19,[7] the Court orally denied the first request as moot because the government had agreed to produce the unredacted Warrants and their supporting application, *see id.* at 2:7-12. As to the second request, in light of the government's disclosure of the existence of the Apptix Warrant, counsel for Mr. Archer requested that the Court order the government to "segregate and not review" the contents of the Apptix production until further order of the Court. *Id.* at 2:23-3:3. The Court denied this request, as well as Mr. Archer's original request that the Court enjoin Google from making a production responsive to the Google Warrant. *See id.* at 17:23-24.

In so doing, the Court agreed with the government that Mr. Archer should not be able to challenge the Warrants prior to their execution because suppression after the fact was an appropriate remedy. Echoing the government, the Court held:

> Mr. Archer and Mr. Cooney are essentially asking me to set a precedent for staying the execution of all warrants of this nature, to allow a potential pre-execution motion, a proposition for which they offer no authority in this circuit and which I'm not prepared to adopt today. The magistrate judge has deemed these warrants to be proper, and Mr. Archer and Mr. Cooney will have ample opportunity to challenge the validity of the warrants and the manner in which the government conducts its search. As [the prosecutor] noted, *the risk is on the government.* I am not willing at this time to take the novel step of blocking the execution of these warrants.

---

[7] In full, the government stated:

> To the extent that there are privileged communications, we take [defense counsel] obviously at his word that there are, and we are happy to run whatever lawyers' names defense proffers through and segregate those things. *Ultimately, the risk is on the government.* If it turns out that that gives rise to a suppression motion because [counsel] doesn't like the way it's been done, then he can bring that motion, but we are not willing to agree to [allow Mr. Archer to challenge the Warrants prior to their execution]. We don't think it's appropriate, and *if that risk is on the government, then that risk is on the government.*

Decl. Ex. 9 at 16:15-24 (emphases supplied).

Id. at 18:13-24 (emphasis supplied).

2. In The Court Of Appeals

Mr. Archer immediately sought a stay pending appeal of the Court's decision, *see* Decl. Ex. 10, which this Court denied for largely the same reasons, s*ee* Decl. Ex. 11, at 2 (holding that Mr. Archer "can seek to suppress those materials, request a taint hearing, or even ask the Court to disqualify members of the Government team who encountered the materials").

Shortly thereafter, Mr. Archer sought a stay from the Second Circuit, along with a writ of mandamus. *See* Decl. Exs. 12-13. After the Court of Appeals granted a temporary stay, the government filed its response. *See* Decl. Ex. 14-15. As before, the focus of the government's opposition was that Mr. Archer had numerous other potential avenues for obtaining the relief that he sought, chief among them moving to suppress the fruits of the Warrants prior to trial. *See, e.g.*, Decl. Ex. 15 ¶¶ 22, 29, 40, 45. The Court of Appeals ultimately agreed, finding that it "lack[ed] jurisdiction over [Mr. Archer's] appeal[] because a final order ha[d] not been issued by the district court," Decl. Ex. 16. The panel therefore dismissed Mr. Archer's appeal and denied his emergency motion as moot. *See id.* The Second Circuit likewise denied Mr. Archer's mandamus petition, finding that he had "not demonstrated that he lack[ed] an adequate, alternative means of obtaining [the] relief" he sought. *See* Decl. Ex. 17. Thus, the Court of Appeals, like this Court, declined to pass on the merits of Mr. Archer's challenge to the Warrants.

E. Discussions Between The Parties

On April 3, 2017, counsel for Mr. Archer had a telephone call with the government during which the government stated that Google had produced information responsive to the Google Warrant. The government also outlined its intention to take the following steps to review the fruits of both Warrants for privilege:

1. Run a list of search terms provided by counsel for Messrs. Archer and Momtazi to segregate potentially privileged documents.

2. Have a "wall" AUSA review the potentially-privileged materials.

3. If the "wall" AUSA determines that certain material is not privileged, that material will be released to the prosecution team. If the "wall" AUSA determines that certain material is privileged, that material will be withheld from the prosecution team. If the "wall" AUSA has questions about whether certain material is privileged, he or she will "seek guidance."

Decl. Ex. 18 at 3. The government also suggested that "the wall AUSA may 'seek guidance' from the prosecution team itself." *Id.*

On April 6, 2017, Mr. Archer responded in writing to emphasize his "profound concerns regarding the government's invasion" of thousands of his attorney-client privileged communications, and to continue the dialogue on the exact procedures that would be put in place "to safeguard [his] privilege and ensure that privileged information does not taint the continued litigation of this case." *Id.* at 1.[8] Mr. Archer's letter referenced the government's representations before the Court at the January 31, 2017 conference and before the Second Circuit that it would work with Mr. Archer to devise a review protocol. *See id.* at 2 (quoting Decl. Ex. 9 at 16:25-17:8; Decl. Ex. 15 ¶ 41). The letter also referenced the government's recognition "that it will bear the consequences of failing to appropriately ensure that Mr. Archer's privilege is not breached," quoting both the commitment the government made before the Court at the January 31, 2017 conference and the portion of the Court's holding that was expressly predicated on that commitment. *See id.* (quoting Decl. Ex. 9 at 16:15-24, 18:21-22).

[8] Mr. Archer's April 6, 2017 letter explicitly stated that he did "not in any way waive his right to challenge the appropriateness of the [W]arrants or to seek to suppress the use of any evidence derived, directly or indirectly, from them, including on the grounds that privileged materials have tainted the prosecution." Decl. Ex. 18 at 1-2.

Mr. Archer's letter also outlined for the government potential problems with its contemplated review protocol. *See id.* at 3-5. In addition to citing "a number of courts [that] have criticized the practice of using a 'wall' AUSA to conduct a privilege review," Mr. Archer insisted that (1) "anyone exposed to privileged material be entirely isolated from the prosecution team, meaning that they do not come from the same office or report to the same supervisors"; (2) when the wall AUSA "seek[s] guidance," he or she must seek such guidance from a pre-designated individual to whom the same standards of isolation from the prosecution team apply, and must not seek guidance from the prosecution team itself, which the government had suggested the wall AUSA might do; and (3) the wall AUSA must not "be tasked with deciding whether the so-called 'crime-fraud exception' applies to otherwise privileged documents," which the government had suggested could be part of his or her role. *Id.*

Mr. Archer then reiterated his "request that the government document its review protocol *in writing* so that there is no ambiguity about how the government has decided to undertake and actually conducted the review." *Id.* at 5 (emphasis in original). Specifically, Mr. Archer took the position that, "[a]t a minimum the government should document, *in writing*, the following":

> a. The terms and methodology used to isolate potentially privileged documents from presumptively non-privileged ones.
>
> b. The review protocol as adopted, and the complete set of instructions and information given to the wall AUSA to follow in conducting his or her review, including the procedures for how and from whom to "seek guidance."
>
> c. The contents and other particulars of any communications between the wall AUSA and anyone else on the subject of the review, including supervisors. . . .
>
> d. The manner in which the wall AUSA conducts his or her review, including his or her decision about which documents are privileged or non-privileged, and why.

Id. (emphasis in original). The letter also stated that, "[i]n the event that the government chooses to permit the wall AUSA to speak to the prosecution team or its supervisors – something that we reiterate should never happen – those communications themselves should all be in writing so that they are clear and unambiguous." *Id.*

Mr. Archer's letter also proposed an alternative review protocol that would have permitted him to conduct the privilege review himself, just as he would in responding to a subpoena. Mr. Archer's proposed review protocol was modeled after the protocol adopted by the Sixth Circuit when faced with similar circumstances in *In re Grand Jury Subpoenas*, 454 F.3d 511 (6th Cir. 2006). *See* Decl. Ex. 18 at 5-7.[9] Specifically, Mr. Archer proposed that:

> 1. [His] counsel [would] run [an] attached [list of] search terms (which were compiled jointly by [his] and Mr. Momtazi's lawyers) against the information produced by Google and Apptix to identify potentially-privileged documents. The documents would then be split into two batches: those that hit on the search terms, and those that did not.[10]
>
> 2. Any document that does not hit on one of the search terms [would] be immediately produced to the government to review, subject to the terms of the warrants. . . .
>
> 3. [His] counsel would conduct a privilege review of those documents that do hit on one or more of the search terms:

---

[9] *In re Grand Jury Subpoenas* obviously involved subpoenas, rather than a search warrant. The government itself has acknowledged, however, that a warrant issued pursuant to the Stored Communications Act functions as a "hybrid" between a subpoena and a search warrant. *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 214 (2d Cir. 2016) (noting that the government had urged the court to follow an approach "that would treat the SCA warrant as equivalent to a subpoena"). An SCA warrant's subpoena-like characteristics – insofar as they compel a service provider to gather and produce responsive records, rather than authorize federal agents to seize the evidence themselves – are particularly relevant to issues surrounding the government's privilege review.

[10] The list of search terms attached to Mr. Archer's letter included the names and other identifiers of individual lawyers, legal personnel, and law firms, as well as several other terms designed to identify potentially privileged material, such as terms designed to capture phrases like "Attorney Client Privileged" and "Attorney Work Product" that often appear in privileged communications. *See* Decl. Ex. 18 at 8-9.

> a. Any documents . . . determine[d] to be non-privileged [would] be produced to the government to review, subject to the terms of the warrants.
>
> b. Any documents . . . determine[d] to be partially privileged [would] be appropriately redacted, and the redacted version produced to the government to review, subject to the terms of the warrants.
>
> c. Any document . . . determine[d] to be privileged [would] be withheld and put on a privilege log. . . .
>
> 4. In the event that the government believe[d] that a document ha[d] been wrongly withheld as privileged, the parties [would] meet and confer and/or the government [could] challenge the designation in court.

Id. at 5-6. Mr. Archer's letter also stated his willingness "to discuss having the Court employ a Special Master to run the search terms and separate the two batches of documents, if the government believes that is necessary," *id.* at 6 n.3 (citing *In re Grand Jury Subpoenas*, 454 F.3d at 524), and his belief "that potentially relevant documents should be isolated before any privilege analysis is performed in order to avoid unnecessary time and expense analyzing irrelevant documents for privilege," *id.* at 6 n.4.

The government responded by e-mail to Mr. Archer's letter the next day, April 7, 2017. *See* Decl. Ex. 19. The government took issue with one individual referenced in Mr. Archer's list of search terms and asked, "[w]ith regard to the other names of individuals on your list, (1) for each attorney (or other law firm personnel) please identify the law firm with which the individual is affiliated; and (2) for any non-attorney/non legal personnel please provide a justification for their inclusion in the proposed list of search terms." *Id.* The government did not otherwise respond to any of the proposals or points made in Mr. Archer's letter. On April 12, 2017, counsel for Mr. Archer provided answers to all of the government's questions. *See* Decl. Ex. 20.

In the end, the government not only rejected Mr. Archer's proposed review protocol, it also declined to use the search terms that Mr. Archer provided. Instead, according to the

government, it ran search terms using only the proper names and e-mail addresses of lawyers identified by Mr. Archer. *See* Decl. Ex. 21 at 2 n.3. In refusing to use commonly-employed phrases like "Attorney-Client Privileged" or "Privileged and Confidential," the government absolutely ensured that its privilege screen would not pick up privileged communications with lawyers whose names did not appear on Mr. Archer's list.[11]

F. The Government Produces To All Defendants The Entire Contents Of The Targeted Accounts Other Than Certain Documents Segregated For Privilege Review, Including Approximately 70,000 Admittedly Non-Responsive Documents

The government finally began producing documents responsive to the Warrants in late July 2017. *See* Decl. Ex. 22. Based on a cursory manual review shortly after receipt of only the first 2,000 pages of over 500,000 pages of material produced by the government, Mr. Archer's counsel was able to determine that the government had "made absolutely no effort to adhere to the restrictions" in the Warrants, and had instead "seized and produced to co-counsel – without even a protective order to shield private information – thousands upon thousands of pages of irrelevant, privileged, personal, and business confidential information." Decl. Ex. 21 at 2-3 & n.4.

On July 25, 2017, Mr. Archer raised his concerns with the government, and asked the government to confirm whether it had done a responsiveness review prior to production. *See id.* at 12-13. Assuming, based on what he had seen in the production, that it had not done any responsiveness review, Mr. Archer requested that the government "require the other defendants to return all copies of the documents from the accounts associated with [him], to be replaced

[11] Even with respect to proper names, it is not clear what search terms the government employed. For example, to search for the lawyer Jane Doe, Mr. Archer does not know if the government searched only for "Jane Doe," or if it also searched for variations and related terms designed to pick up all privileged communications (*e.g.*, "Doe, Jane," "J. Doe," "Jane D," "Doe & Smith LLC," "jane@doesmith.com," etc.).

with only documents that are actually responsive" to the Warrants. *Id.* at 12. The government responded by confirming that it had produced non-responsive documents as well as responsive documents, but stated that it did not believe that a request to "claw back any non-responsive emails is appropriate." *Id.*

On July 26, 2017, Mr. Archer was forced to file an emergency application requesting that the Court "issue an order requiring all defendants to return or destroy" the government's production of the fruits of the Warrants. *Id.* at 1. Mr. Archer listed several examples of plainly non-responsive documents found in the production during his cursory manual review, including, among other things, privileged communications solely between Mr. Archer and his wife on incredibly sensitive topics, contact information for at least one high-profile public figure, and confidential business and financial information about companies and investments entirely unrelated to this case. *See id.* at 3-4. Based on these documents alone, it was clear that the government had "made no effort to comply with the Warrant[s], instead seizing [Mr. Archer's] account data whole-hog and producing it to all of the parties in this litigation," and that "[t]he government's utter and unapologetic disregard for the language of the Warrant[s] ha[d] transformed what was already an overbroad search into a warrantless one rendering any materials collected subject to suppression." *Id.* at 4, 6 (citing *United States v. Liu*, 239 F.3d 138, 140 (2d Cir. 2000) (wholesale suppression of the fruits of a search is justified when the agents executing a warrant "effect a 'widespread seizure of items that were not within the scope of the warrant' . . . and . . . do not act in good faith . . . ." (citations omitted)).

In response, the government claimed that it believed it had obtained Mr. Archer's consent to producing the undifferentiated contents of his e-mails, and asked the Court to determine whether the government possessed the entirety of Mr. Archer's e-mails for *Brady* purposes. *See* Decl. Ex. 23 at 1. The government asked that the Court deny Mr. Archer's application if the

Court determined that it was "in possession" of such documents, and stated that, if the Court determined that it was not "in possession" of such documents, it would have no objection to Mr. Archer's request "that the full email production be replaced by a production solely of responsive documents." *Id.*

The government's response also provided the following explanation of the manner in which its review of the fruits of the Warrants was proceeding, much of which Mr. Archer learned for the first time upon reading it:

> The Government used the list of attorneys and law firms [provided by Mr. Archer] to segregate all potentially privileged documents for review by a wall AUSA. On July 3, 2017, the potentially privileged emails having been segregated for review, the trial team first received access to the non-privileged emails obtained pursuant to the Warrant, consisting of approximately 130,000 documents. . . . [T]he Government then embarked on a "responsiveness" review in order to identify emails that fell within the category of documents sought by the Warrant[s]. The trial team used a detailed list of search terms to assist in identifying responsive documents. The use of the "responsiveness" search terms yielded approximately 58,000 potentially responsive emails. Non-privileged emails which did not hit on a search term, of which there are approximately 70,000[,] were deemed non-responsive and will not be further reviewed by the Government absent an additional warrant from the Court. The 58,000 potentially responsive emails that did hit on the responsiveness search terms are being further reviewed for a final determination as to responsiveness. That review is ongoing and at the completion of the responsiveness review process, the Government will produce to each of the defendants the universe of emails that are deemed responsive to the Warrant[s].

Id. at 2. The government's July 2017 production, then, included not only the approximately 58,000 documents that "hit on the responsiveness search terms" – which search terms the government has never disclosed to Mr. Archer – but also the approximately 70,000 documents that did not hit on any search terms and which "were deemed non-responsive" by the government even before they were produced. *Id.*

On August 3, 2017, the Court granted Mr. Archer's motion, finding that the government "produced all of the materials obtained pursuant to the warrant . . . without regard to responsiveness. Many of these documents have no relevance to the facts of this case and are personal and/or confidential in nature." Decl. Ex. 24 at 4:13-17. The Court therefore ordered the defendants to return or destroy the government's production, and ordered the government "to replace this production with a new production consisting solely of materials responsive to the warrant[s]." *Id.* at 13:11-14:3.[12]

* * *

In the intervening several months, Mr. Archer has been able to conduct a more thorough review of the contents of the Archer Accounts produced by the government in July 2017. This search has revealed far more extreme and shocking violations of his personal privacy than did the cursory manual review of the first 2,000 pages of material referenced above. To cite but a handful from among literally thousands upon thousands of examples, the government's production to Mr. Archer *and all of his co-defendants* included the following highly personal, sensitive, and/or confidential – but totally irrelevant – e-mails:

- Approximately 750 e-mails plainly subject to the marital privilege, including e-mails:
  - relating to Mr. Archer and his wife's children, their children's medical issues, and their family's childcare arrangements,
  - attaching copies of family medical documents, one of Mr. Archer's children's birth certificates, and one of Mr. Archer's children's report cards,
  - relating to the status of Mr. Archer's wife's pregnancy and discussing possible names for the baby,

[12] The Court subsequently modified its order to allow Mr. Archer to keep the materials obtained from his own e-mail accounts. *See* Decl. Ex. 25.

  - attaching family pictures,
  - discussing the strain created by Mr. Archer's busy travel schedule,
  - relating to a construction loan that Mr. Archer's wife was considering, and various construction and interior design projects at Mr. Archer's home, including plans for home security,
  - attaching a Valentine's Day card to Mr. Archer from his wife,
  - relating to Mr. Archer's wife's efforts to obtain a service dog for a family member,
  - discussing Mr. Archer and his wife's charitable donations,
  - containing and/or attaching insurance information and documents, and
  - discussing various contemplated real estate investments;
- Discussions regarding Mr. Archer's wife planning home renovations;
- Discussions regarding personal plans with parties unrelated to this case;
- Discussions regarding charity events that Mr. Archer and his wife were involved with;
- Discussions regarding events at the school of Mr. Archer's young son; and
- Discussions regarding Mr. Archer's young son's flag football league.

Decl. ¶ 31.

Moreover, the government's production also included a number of attorney-client privileged documents that, just as Mr. Archer had foreseen, evaded the government's wholly insufficient initial screening for such materials. For example, the government failed to screen out privileged communications between Mr. Archer and his counsel dating from after the

beginning of the investigation in this matter, which related to ongoing negotiations with the government and SEC over producing documents. *See* Decl. ¶ 30.

G. The Government's Production Of Purportedly Responsive Documents

Beginning in late August 2017, the government finally started to produce documents that were purportedly responsive to the Warrants. Thus far, the government has made a total of eight productions of materials responsive to the Warrants, comprising a total of approximately 10,000 documents – a far cry from the almost 130,000 documents it had previously produced, and less than one-fifth of the 58,000 so-called "preliminarily responsive" documents that purportedly hit on the government's secret list of responsiveness search terms. Decl. ¶ 42. The government made its most recent production on or about January 10, 2018. *Id.*

LEGAL STANDARD

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. "The text of the Amendment thus expressly imposes two requirements. First, all searches and seizures must be reasonable. Second, a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." *Kentucky v. King*, 563 U.S. 452, 459 (2011) (citing *Payton v. New York*, 445 U.S. 573, 584 (1980)).

The Supreme Court has held that the "essential purpose of the Fourth Amendment [is] to shield the citizen from unwarranted intrusions into his privacy," and that "[t]his purpose is realized by Rule 41 of the Federal Rules of Criminal Procedure, . . . which implements the

Fourth Amendment." *Jones v. United States*, 357 U.S. 493, 498 (1958).[13] "It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment." *Payton*, 445 U.S. at 583; *see also Ashcroft v. al-Kidd*, 563 U.S. 731, 742 (2011) ("The Fourth Amendment was a response to the English Crown's use of general warrants, which often allowed royal officials to search and seize whatever and whomever they pleased while investigating crimes or affronts to the Crown."); *Arizona v. Gant*, 556 U.S. 332, 345 (2009) ("[T]he central concern underlying the Fourth Amendment [is] the concern about giving police officers unbridled discretion to rummage at will among a person's private effects.").

As the Supreme Court has held, there are

> two distinct constitutional protections served by the warrant requirement. First, the magistrate's scrutiny is intended to eliminate altogether searches not based on probable cause. The premise here is that any intrusion in the way of search or seizure is an evil, so that no intrusion at all is justified without a careful prior determination of necessity. The second, distinct objective is that those searches deemed necessary should be as limited as possible. Here, the specific evil is the 'general warrant' abhorred by the colonists, and the problem is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings. The warrant accomplishes this second objective by requiring a 'particular description' of the things to be seized.

Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) (citations omitted). In other words, "the Warrants Clause requires particularity and forbids overbreadth." *United States v. Cioffi*, 668 F.Supp.2d 385, 390 (E.D.N.Y. 2009); *accord In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled*

[13] Although the Warrants called for information in the possession of third parties (Google and Apptix), there is no doubt that Mr. Archer had a legitimate privacy interest in the Archer and Momtazi Accounts, as the Bieniek Affidavit recognized that Mr. Archer was the user of the Archer Accounts and that Momtazi, Mr. Archer's employee, was the user of the Momtazi Accounts. *See* Decl. Ex. 4 at 12.

By Google, Inc., 33 F. Supp. 3d 386, 389 (S.D.N.Y. 2014), as amended (Aug. 7, 2014); *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 450 (S.D.N.Y. 2013).

"Although somewhat similar in focus, these are two distinct legal issues: (1) whether the items listed as 'to be seized' in the warrant were overbroad because they lacked probable cause and (2) whether the warrant was sufficiently particularized on its face to provide the necessary guidelines for the search by the executing officers." *United States v. Hernandez*, No. 09-cr-625, 2010 WL 26544, at *7 (S.D.N.Y. Jan. 6, 2010) (citations omitted); *see also United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006) ("Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." (citation omitted)). Thus, "a warrant can violate the [Warrants Clause] 'either by seeking specific material as to which no probable cause exists, or by giving so vague a description of the material sought as to impose no meaningful boundaries.'" *Cioffi*, 668 F. Supp. 2d. at 390 (quoting *United States v. Cohan*, 628 F. Supp. 2d 355, 359 (E.D.N.Y. 2009)).

A. The Fourth Amendment's Prohibition On Overbreadth

"The prohibition on overbreadth necessitates that 'the scope of the warrant be limited to the probable cause on which the warrant is based.'" *United States v. Tairod Nathan Webster Pugh*, No. 1:15-cr-00116 (NGG), 2015 WL 9450598, at *19 (E.D.N.Y. Dec. 21, 2015) (quoting *Hernandez*, 2010 WL 26544, at *7). "In determining whether a warrant is overbroad, courts must focus on 'whether there exists probable cause to support the breadth of the search that was authorized.'" *Zemlyansky*, 945 F.Supp.2d at 464 (quoting *Hernandez*, 2010 WL 26544, at *8). "If the breadth of the search exceeds the probable cause on which that search was based, the government runs afoul of the Fourth Amendment." *United States v. Feng Ling Liu*, No. 12-cr-934 (RA), 2014 WL 101672, at *7 (S.D.N.Y. Jan. 10, 2014). In other words, as the Second

Circuit has stated, "'an otherwise unobjectionable description of the objects to be seized is defective if it is broader than can be justified by the probable cause upon which the warrant is based.'" *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013) (quoting 2 W. LaFave, Search and Seizure § 4.6(a) (5th ed. 2012)).

Probable cause, in turn, is "a fluid concept – turning on the assessment of probabilities in particular factual contexts – not readily, or even usefully, reduced to a neat set of legal rules." *Illinois v. Gates*, 462 U.S. 213, 232 (1983). It exists if, "given all the circumstances set forth in the affidavit, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Id.* at 238; *see also United States v. Falso*, 544 F.3d 110, 117 (2d Cir. 2008). And while a magistrate's determination that probable cause exists to support the issuance of a search warrant "should be paid great deference by reviewing courts," *Gates*, 462 U.S. at 236, it is for the reviewing court to "decide whether the magistrate performed his neutral and detached function on the facts before him, and did not merely serve as a rubber stamp for conclusions drawn by the police," *United States v. Travisano*, 724 F.2d 341, 345 (2d Cir. 1983). As the Supreme Court emphasized in *Gates*, a warrant affidavit "must provide the magistrate with a substantial basis for determining the existence of probable cause, and . . . wholly conclusory statement[s] . . . fail[] to meet this requirement." 462 U.S. at 239. "In order to ensure that . . . an abdication of the magistrate's duty does not occur," the Supreme Court has instructed that courts must "conscientiously review the sufficiency of affidavits on which warrants are issued." *Id.*

B. The Fourth Amendment's Particularity Requirement

Separate and apart from the prohibition on overbreadth, the particularity requirement requires "that the warrant must clearly state what is sought." *Cioffi*, 668 F.Supp.2d at 390 (quotations omitted). Particularity concerns arise when a warrant's description of the place to be searched or the items to be seized "is so vague that it fails reasonably to alert executing officers

to the limits" of their search and seizure authority. *United States v. Clark*, 638 F.3d 89, 94 (2d Cir. 2011) (citation omitted). To satisfy the particularity requirement, a warrant "must be sufficiently specific to permit the rational exercise of judgment by the executing officers in selecting what items to seize." *Liu*, 239 F.3d at 140 (quotations and alterations omitted).

The particularity requirement has three components. "First, a warrant must identify the specific offense for which the police have established probable cause." *Galpin*, 720 F.3d at 445 (citations omitted). "Second, a warrant must describe the place to be searched." *Id.* at 445-46 (citations omitted). "Third, the warrant must specify the 'items to be seized by their relation to designated crimes.'" *Id.* at 446 (quoting *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010); citing *United States v. Buck*, 813 F.2d 588, 590-92 (2d Cir. 1987) (finding that a warrant authorizing the seizure of "any papers, things or property of any kind relating to [the] previously described crime" failed the particularity requirement because it "only described the crimes – and gave no limitation whatsoever on the kind of evidence sought")).

As the Supreme Court has recognized, document searches pose unique Fourth Amendment concerns:

> [T]here are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable. In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. . . . [R]esponsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.

Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).

"The dawn of the Information Age has only heightened those concerns." *Cioffi*, 668 F. Supp. 2d at 391. "The risk of exposing intimate (and innocent) correspondence to prying eyes is

magnified because '[c]omputers . . . often contain significant intermingling of relevant documents with documents that the government has no probable cause to seize.'" *Id.* (quoting *United States v. Vilar*, No. 05-cr-621 (KMK), 2007 WL 1075041, at *35 (S.D.N.Y. Apr. 4, 2007)). As the Second Circuit explained in the parallel context of digital searches of computer hard drives:

> Where . . . the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance. As numerous courts and commentators have observed, advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain. *See United States v. Payton*, 573 F.3d 859, 861-62 (9th Cir. 2009) ("There is no question that computers are capable of storing immense amounts of information and often contain a great deal of private information. Searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers."); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (noting [a] computer's potential "to store and intermingle a huge array of one's personal papers in a single place"); Orin Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 569 (2005) (Computers "are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more."). The potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous. This threat is compounded by the nature of digital storage. Where a warrant authorizes the search of a residence, the physical dimensions of the evidence sought will naturally impose limitations on where an officer may pry: an officer could not properly look for a stolen flat-screen television by rummaging through the suspect's medicine cabinet, nor search for false tax documents by viewing the suspect's home video collection. Such limitations are largely absent in the digital realm, where the size or other outwardly visible characteristics of a file may disclose nothing about its content.

Galpin, 720 F.3d at 446-47; *see also In the Matter of a Warrant*, 33 F. Supp. 3d at 394 ("We perceive no constitutionally significant difference between the searches of hard drives . . . and searches of email accounts.").

There is therefore "'a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.'" *Galpin*, 720 F.3d at 447 (quoting *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc and per curiam)). "This threat demands a heightened sensitivity to the particularity requirement in the context of digital searches." *Id.*; *see also United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) ("The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important.").

ARGUMENT

THE FRUITS OF THE WARRANTS SHOULD BE SUPPRESSED

I. THE WARRANTS ARE FACIALLY DEFECTIVE BECAUSE THEY AUTHORIZED AN UNCONSTITUTIONAL GENERAL SEARCH

The fruits of the Warrants must be suppressed for a very simple reason: the Warrants on their faces authorize a search for "evidence of crime" without any further restriction. This precise formulation has been found, over and over, to constitute an unconstitutional general search.

"There is . . . one form of particularity whose absence the Second Circuit has unequivocally and unqualifiedly condemned: '[A]uthorization to search for evidence of a crime, that is to say, any crime, is so broad as to constitute a general warrant.'" *Cioffi*, 668 F. Supp. 2d at 392 (quoting *United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992) ("Mere reference to 'evidence' of . . . general criminal activity provides no readily ascertainable guidelines for the executing officers as to what items to seize." (alteration in original))). "Thus, where a warrant does not, either on its face or via incorporation of a supporting affidavit, 'limit the items to be

seized from [a defendant's] personal email account to emails containing evidence of the crimes charged in the indictment,' the warrant will not be considered constitutionally valid." *United States v. Patel*, No. 16-cr-798 (KBF), 2017 WL 3394607, at *4 (S.D.N.Y. Aug. 8, 2017) (quoting *Cioffi*, 668 F. Supp. 2d at 396 (alteration in original)); *see also Galpin*, 720 F.3d 436, 447-48 ("The district court determined, and the government does not dispute, that insofar as the warrant generally authorized officers to search Galpin's physical property and electronic equipment for evidence of violations of 'NYS Penal Law and or Federal Statutes,' the warrant violated the Fourth Amendment's particularity requirement." (citing *United States v. Rosa*, 626 F.3d 56, 62 (2d Cir. 2010) (warrant authorizing seizure of electronic equipment without specifying the legal violation "provided [officers] with no guidance as to the type of evidence sought" and constituted a general warrant); *United States v. Burgess*, 576 F.3d 1078, 1091 (10th Cir. 2009) ("If the warrant is read to allow a search of all computer records without description or limitation it would not meet the Fourth Amendment's particularity requirement.")).

Here, on their faces, the Warrants explicitly allow the government to search for "evidence of crime" related to *any* criminal offense and "communications constituting" *any* criminal offense. Decl. Ex. 5 at 9-10, 16-17. Specifically, the Warrants' operative language provides, in pertinent part, as follows:

> *Law enforcement personnel . . . are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of* Title 18, United States Code, Section 1348, and Title 15, United States Code, Sections 78j(b) and 78ff, Title 17, Code of Federal Regulations, Sections 240.10b-5; conspiracy to commit securities fraud, in violation of Title 18, United States Code, Section 371; investment advisor fraud, in violation of Title 15, United States Code, Sections 80b-6 and 80b-17; and conspiracy to commit investment adviser fraud, in violation of Title 18, United States Code, Section 371, *among other statutes, including the following:*
>
> * * *

> - *evidence of crime* (*e.g.*, agreement to engage in unlawful conduct, references to or discussion of unlawful conduct), *communications constituting crime* (*e.g.*, emails containing fraudulent representations) . . .

Id. (emphases supplied). As a matter of straightforward grammar, therefore, the Warrants authorized the government to search for and seize "evidence of crime" relating to four specified statutes, "among other statutes." In other words, the Warrants list the four crimes charged in the Indictment, which the Bieniek Affidavit defines as the "Subject Offenses," *as mere examples* of the types of crimes for which "[l]aw enforcement personnel . . . are authorized to review the records produced by" Google and Apptix "to locate any evidence . . . of violations of . . . other statutes." *See* Decl. Ex. 5, at 9, 16.

The Second Circuit has expressly held that this formulation is unconstitutional. In *Galpin*, the warrant affidavit purported to provide probable cause in connection with the defendant's failure to register as a sex offender under N.Y. Correction Law § 168–f. The warrant, however, authorized the government to search for "evidence that will constitute, substantiate or support violations of NYS Corrections Law, section 168–f subdivision four, *NYS Penal Law and or Federal Statutes*." 720 F.3d at 441 (emphasis supplied). The Second Circuit held – and indeed the government in that case conceded – that the warrant's specific reference to N.Y. Correction Law § 168–f could not modify or save the more general language, which allowed the government to search for "evidence that will constitute, substantiate or support violations of . . . NYS Penal Law and or Federal Statutes." *Id.* at 447 ("we agree that the warrant was facially overbroad and thus violated the Fourth Amendment."). Similarly, the Warrants' reference in this case to the offenses charged in the Indictment cannot save the simple fact that they authorized the government to search for "evidence of crime," not only of the charged

offenses but also any "other statutes."[14] *See also United States v. Roche*, 614 F.2d 6, 8 (1st Cir. 1980) (affirming grant of suppression and rejecting government's claim that warrant was sufficiently particular because it limited the search to evidence in violation of the mail fraud statute); *United States v. Maxwell*, 920 F.2d 1028, 1033 (D.C. Cir. 1990) (finding that warrant that permitted search for evidence of wire fraud was "fatally overbroad," and holding that "[r]eferences to broad statutes realistically constitute no limitation at all on the scope of an otherwise overbroad warrant and therefore cannot save it.")

"[I]t is obvious that a general warrant authorizing the seizure of 'evidence' without mentioning a particular crime or criminal activity to which the evidence must relate is void under the Fourth Amendment." *George*, 975 F.2d at 77 (citations omitted). While the Warrants here mention the four crimes charged in the Indictment as *examples* of the crimes for which law enforcement personnel should search for evidence, fruits, and instrumentalities, they do not state that such evidence, fruits, and instrumentalities "must" relate to those crimes. *Id.* To the contrary, both Warrants explicitly provide that law enforcement personnel may search the full breadth of documents, information, and data produced by Google and Apptix for any "evidence of crime" or "communications constituting crime" relating to literally any violations of any

[14] As in *Galpin*, the Warrants include specific examples of the types of material that fall within their scope, but that cannot save their overbreadth. *Compare, e.g.*, 720 F.3d at 441 (authorizing seizure of "Any and all photographs depicting sexual conduct by a child and/or minors engaged in sexually explicit conduct"), *with* Decl. Ex. 5, at 9, 16 (listing, for example, "evidence of the agreement to engage in a fraudulent scheme involving the issuance of bonds on behalf of the [WLCC] and the misappropriation of the proceeds of those bonds"). Listed conspicuously among those more particularized examples of the "evidence, fruits, and instrumentalities" that law enforcement personnel may attempt "to locate" pursuant to the Warrants, however, are the examples of "evidence of crime" and "communications constituting crime," which are left entirely general and not tied to either the facts of this case or the elements of the Subject Offenses. Decl. Ex. 5 at 9-10, 16-17. The Warrants' other examples are likewise entirely generic and unparticularized. *See id.* at 10, 17 (providing "agreement to engage in unlawful conduct" and "references to or discussion of unlawful conduct" as examples of "evidence of crime" and "emails containing fraudulent representations" as an example of "communications constituting crime").

criminal statutes, including, but not limited to, the four charged offenses. *See* Decl. Ex. 5 at 9-10, 16-17. *See generally Cioffi*, 668 F. Supp. 2d at 389 ("There was no provision limiting the emails to be seized to those containing evidence of the crimes charged in the indictment.").

The Warrants are therefore effectively limitless, *see Clark*, 638 F.3d at 94 (noting that particularity concerns arise "where the description in the warrant of the place to be searched is so vague that it fails reasonably to alert executing officers to the limits of their search authority" (citation omitted)), as they fail to meet two of the three particularity requirements – *i.e.*, that "a warrant must identify the specific offense for which the police have established probable cause" and "must specify the items to be seized by their relation to designated crimes," *Galpin*, 720 F.3d at 445-46 (quotation and citation omitted); *see also Mink v. Knox*, 613 F.3d 995, 1010 (10th Cir. 2010) ("warrants for computer searches must *affirmatively limit* the search to evidence of specific . . . crimes" (quotation omitted and alteration and emphasis in original)).

Accordingly, the Warrants are constitutionally defective "general warrants," and their fruits must be suppressed in their entirety. *See, e.g.*, *George*, 975 F.2d at 76 ("authorization to search for 'evidence of a crime,' that is to say, any crime, is so broad as to constitute a general warrant"); *Patel*, 2017 WL 3394607, at *4 ("where a warrant does not . . . limit the items to be seized from a defendant's personal email account to emails containing evidence of the crimes charged in the indictment, the warrant will not be considered constitutionally valid" (quotation and alteration omitted)); *Rosa*, 626 F.3d at 62 (warrant authorizing seizure of electronic devices without specifying the legal violation "provided [officers] with no guidance as to the type of evidence sought" and constituted a constitutionally impermissible general warrant).

II. THE WARRANT AFFIDAVIT FAILED TO SUPPLY PROBABLE CAUSE

For the reasons just given, the Court need look no further than the face of the Warrants to suppress any and all evidence derived from them. But the fruits of the Warrants must be

suppressed for several additional and independent reasons as well, including that the Bieniek Affidavit fails in several ways to supply probable cause.[15]

A. The Affidavit Relied On Stale Evidence

Every single one of the e-mails relied upon in the Bieniek Affidavit was sent more than two years before the Warrants were issued on December 28, 2016. *See* Decl. Ex. 4 at 12-17 (citing e-mails from February, April, May, July, August, September, and October 2014). The allegations regarding Mr. Archer's conduct are likewise dated, as they concern a September 2014 funds transfer and certain alleged communications in October 2014. *See id.* at 15-16. Indeed, nowhere in the Bieniek Affidavit is there any reference to anyone's conduct post-dating October 2014, let alone any post-October 2014 connection to any of the Targeted Accounts. Because the Bieniek Affidavit relied on evidence that was long stale at the time the Warrants were sought, it fails to establish probable cause to believe that the Targeted Accounts would contain relevant evidence.

"While there is no bright line rule for staleness, the facts in an affidavit supporting a search warrant must be sufficiently close in time to the issuance of the warrant and the subsequent search conducted so that probable cause can be said to exist as of the time of the search and not simply as of some time in the past." *United States v. Wagner*, 989 F.2d 69, 75 (2d Cir. 1993). Accordingly, "[i]n evaluating probable cause, a magistrate is always required to consider whether the facts adduced in the warrant application 'appear[] to be current, *i.e.*, true at the time of the application,' or whether they have 'become stale.'" *Walczyk v. Rio*, 496 F.3d

[15] In addition to the deficiencies discussed below, the Bieniek Affidavit and the attached Indictment fail to supply probable cause because they do not adequately allege probable cause to believe that Mr. Archer participated in a crime. Mr. Archer's simultaneously filed motion to dismiss the securities fraud charge against him and for a bill of particulars explains why that is so, and Mr. Archer incorporates those arguments here rather than repeat them.

139, 162 (2d Cir. 2007) (quoting *Rivera v. United States*, 928 F.2d 592, 602 (2d Cir. 1991) (alteration in original)); *see also United States v. Enoa*, No. 93-cr-285 (KTD), 1993 WL 404154, at *1 (S.D.N.Y. Oct. 7, 1993) ("[I]f the information contained in the affidavit supporting a search warrant is too remote in time to the issuance of the warrant, probable cause will lapse and invalidate the warrant.") (citing *Wagner*, 989 F.2d at 75).

Here, because *all* of the e-mails and factual allegations on which probable cause to search the Targeted Accounts was purportedly based predate the issuance of the Warrants by more than two years, probable cause for the search was stale, meaning that the Warrants are unsupported by probable cause and therefore constitutionally defective. *See generally United States v. Reyes*, 922 F. Supp. 818, 827 (S.D.N.Y. 1996) ("while there is no bright line for defining staleness, the information necessary to support a finding of probable cause should be no older than one year"); *see also United States v. Raymonda*, 780 F.3d 105, 117 (2d. Cir. 2015) (holding, "on the basis of nine-month-old evidence, [that] it was not enough simply to show that the suspect had at some point accessed thumbnails of child pornography," and that the probable cause stated in the search warrant affidavit was therefore stale); *United States v. Prideaux-Wentz*, 543 F.3d 954, 959 (7th Cir. 2008) ("The four year gap, without more recent evidence, undermines the finding that there was probable cause that the images would be found during the search. Therefore, we find that the evidence relied on to obtain the warrant here was stale, and the warrant lacked probable cause."); *United States v. Doan*, 245 Fed. Appx. 550, 554 (7th Cir. 2007) (table) (finding affidavit to search e-mail account lacked probable cause because it was based on "seventeen-month-old information" and provided no reason to believe evidence would still be in the account).[16]

[16] For the same reasons, the Warrants also suffer from an overbreadth problem. The Warrants authorize the government to seize documents, information, and data from the Archer

B. A Single E-Mail, On Which Mr. Archer Was Copied, Is Not Sufficient To Seize His Entire Google Account

The overall staleness of the probable cause contained in the Bieniek Affidavit is particularly pronounced with respect to the Google Accounts. The sole asserted basis for a sweeping search of Mr. Archer and Mr. Momtazi's Google Accounts – not just e-mails, but twenty-three other categories of data – is a single e-mail from September 2014, on which Mr. Archer was merely cc'd, and to which he is not alleged to have responded. *See* Decl. Ex. 4 at 16 (sole reference to the so-called Archer Seneca Account and Momtazi Seneca Account). In other words, there is no allegation anywhere in the Bieniek Affidavit that any relevant communications were actually sent *from* Mr. Archer's Google Account, and a single e-mail was sent *to* his account from an individual who is not alleged to be a co-conspirator.

Even under the broadest possible conception of probable cause, this single factual assertion – that the Google Account was cc'd on a single communication twenty-six months prior to the issuance of the Warrants – simply cannot provide probable cause to support the seizure of years' worth of documents, information, and data in and associated with the Google Accounts. *See, e.g.*, *United States v. Cordova*, 792 F.3d 1220, 1224 (10th Cir. 2015) (holding that evidence of single transaction twenty-one months prior to search was so insufficient to establish probable cause that evidence would be found in home that officers could not even rely on warrant in good faith); *Wagner*, 989 F.2d at 75 (six-week delay from a single drug purchase at house rendered probable cause supporting warrant to search house stale); *United States v. Coon*, No. 10-cr-110A, 2010 WL 6647779, at *4-5 (W.D.N.Y. Aug. 20, 2010) (evidence that e-mail

---

Accounts all the way through May 11, 2016 – over eighteen months after the Bieniek Affidavit's latest dated allegations regarding those accounts or Mr. Archer. *See* Decl. Ex. 5 at 3, 14. This temporal overbreadth provides yet another independent basis for the suppression of the fruits of the Warrants.

account received child pornography on one occasion almost a year earlier insufficient to provide probable cause); *United States v. Harper*, No. 05-cr-6068L, 2006 WL 2873662, at *7 n.9 (W.D.N.Y. Oct. 6, 2006) ("single controlled purchase" that "had occurred several months earlier . . . failed to demonstrate reason to believe that cocaine would be discovered in the residence several months later" and was therefore "insufficient to establish probable cause"); *see generally In re Grand Jury Subpoena Dated Mar. 20, 2013*, No. 13-mc-189, 2014 WL 2998527, at *11 (S.D.N.Y. July 2, 2014) ("[A] single, vague piece of testimony does not establish probable cause to believe that Doe was engaged in a scheme that extended past Jane Roe.").

C. The Warrants Purport To Authorize The Seizure Of Various Categories Of Documents That The Affidavit Does Not Address At All

The Warrants are also defective because they authorize the government to seize twenty-three categories of documents and data for which the Bieniek Affidavit does not even purport to supply probable cause. This is not simply information peripheral to e-mails, but extensive and incredibly personal information that is stored separately from e-mail, including photographs, Google Docs, Mr. Archer's web history, information about his on-line shopping, and even the contents of his Google Drive, which is a cloud storage service that could host an extraordinary amount of Mr. Archer's private papers. *See* Decl. Ex. 5 at 3-9, 14-15. Other than to describe these categories of information as the sort of thing available from Google – only one of the biggest companies in the world – the Bieniek Affidavit does not mention them at all. *See id.*

"In determining whether a warrant is overbroad . . . courts must focus on whether there exists probable cause to support the breadth of the search that was authorized." *Zemlyansky*, 945 F.Supp.2d at 464 (quotation omitted). This means that a search warrant is only valid insofar as it "rests on a finding that probable cause exists to believe that a crime has been committed and

evidence or instrumentalities of the crime will be found in the place to be searched." *United States v. Goff*, 2016 WL 3264129, at *5 (S.D.N.Y. June 13, 2016).

Applying these standards, this Court must determine whether the Bieniek Affidavit supplied probable cause to support the breadth of the government's search through the many categories of non-email materials in or associated with the Archer Accounts. *See United States v. Wey*, 256 F. Supp. 3d 355, 382 (S.D.N.Y. 2017) ("[A] warrant is overbroad if its description of the objects to be seized is broader than can be justified by the probable cause upon which the warrant is based." (quotation, citation, and alterations omitted)). But the Bieniek Affidavit's showing of probable cause with respect to the Targeted Accounts is based *solely* on e-mails – it does not mention any of the other types of documents, information, or data contained in the non-email areas of the Archer Accounts or otherwise maintained by the account providers in association with those accounts.

Despite the fact that the Warrants' purported probable cause to search the Archer Accounts was based entirely on e-mails to, from, and cc'ing those accounts, the Warrants nevertheless allow the government to seize and search through vast categories of evidence that range far afield from e-mails. The Google Warrant is particularly outrageous in this regard, as it authorizes law enforcement personnel to search through not only the "[e]mail contents" of that account, but also twenty-three other categories of non-email data contained in or associated with the account. Decl. Ex. 5 at 3-9. Among other things, the Google Warrant authorizes a search through Mr. Archer's Google Drive, Google Docs, Google Sheets, and Google Slides content; his address book; his Picasa Web Albums; his web browser history; his Google Alerts; and his Google Payments records, among myriad other categories. *Id.* The Google Warrant provides this authorization despite the fact that there is nothing in the Bieniek Affidavit or the warrant itself, including Attachment A thereto, that would indicate, let alone provide probable cause to

believe, that any of these non-email areas of the Google Account would contain any evidence, fruits, or instrumentalities of any crimes.

Some of these non-email categories encompass an extraordinary breadth of data. Google Drive, for example, allows users up to 15 GB of cloud-based storage (it is essentially Google's version of Dropbox),[17] and the Bieniek Affidavit and Attachment A to the Google Warrant both state as to Picasa Web Albums that "Google provides users with a certain amount of free storage, currently 1 gigabyte, . . . for digital photographs." *Id.* at 5, 50.[18] Google also maintains web browsing history for all activity in its Chrome browser. *See* Google Privacy Policy, https://www.google.com/policies/privacy. But there is nothing in the Bieniek Affidavit, the Google Warrant, or the attachments to the Google Warrant that would supply probable cause to believe that Mr. Archer's browsing history – let alone his Google Payments data, Google URL Shortener data, Google Analytics data, or Google Alerts history, to name but a few examples – would shed any light whatsoever on any of the crimes charged in the Superseding Indictment.[19]

And while the Google Warrant is the far more egregious of the two, the Apptix Warrant is also constitutionally overbroad in the same way. The Apptix Warrant authorizes a search

---

[17] To understand just how much data that is, 15 GB represents more than *ten million* pages of text. *See* "How Many Pages in a Gigabyte?", LexisNexis, available at http://bit.ly/2sJt1mM (providing that 1 GB of data represents approximately 677,963 pages of text, meaning that 15 GB represents 10,169,445 pages of text).

[18] As to Picasa Web Albums, while the Bieniek Affidavit makes the boilerplate and tautological assertion that photos may contain "the identities and locations of co-conspirators or victims," Decl. Ex. 4 at 18, it does not provide any basis for believing that Mr. Archer would have such photographs in his Picasa Web Albums (or anywhere else), or for inferring that defendants accused of committing securities fraud and/or participating in conspiracies to commit securities fraud typically photograph their co-conspirators or victims, or anything else relevant to the crimes they are alleged to have committed.

[19] When the government unlawfully produced the entirety of Mr. Archer's e-mail accounts, it also confirmed that it had in fact seized these various categories of things by producing various documents that came from other (non-email) parts of the Google Accounts. *See* Decl. ¶ 36.

through not only "[e]mail contents," but also Mr. Archer's address book, subscriber and billing information, transactional information, customer correspondence, and preserved records[20] despite the fact that there is simply no showing whatsoever that any of these non-email areas of the Apptix Account would have any relevance to the charged crimes. *Id.* at 58-59. As to customer correspondence, for example, Attachment A to the Apptix Warrant states that Apptix "typically maintain[s] records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account," *id.* at 59, but there is no logical basis for believing that Mr. Archer's correspondence with Apptix about the Apptix Account, or any correspondence between Apptix and any third parties about the Apptix Account, would provide any insight whatsoever into any of the charged crimes. Certainly the Bieniek Affidavit provides none.

The government in this case acknowledged before the Second Circuit that, "[a]s to each category of evidence identified for seizure in the warrant, there must exist probable cause to believe it is relevant to the investigation at issue." Decl. Ex. 15 ¶ 31. As explained above, however, the Warrants simply do not supply probable cause for "each category of evidence" they seek. *Id.* The only category of evidence even addressed by the Bieniek Affidavit is "[e]mail contents" – which is one of six different categories of evidence sought by the Apptix Warrant and one of twenty-four different categories of evidence sought by the Google Warrant. *See* Decl. Ex. 4 at 47-53, 58-59; *see also Armstrong v. City of Melvindale*, 432 F.3d 695, 700 (6th Cir. 2006) ("Though Defendants may have had probable cause to believe the ownership documents would be found on the Melvindale premises, no probable cause existed to believe the documents themselves evidenced a crime. Although Armstrong asserted an ownership interest in the seized

[20] All of these same categories of non-email documents, information, and data were sought by the Google Warrant as well. *See* Decl. Ex. 5 at 3-9.

computers, the officers did not seek to obtain the warrant on the strength of any link between those ownership documents and a crime.").

* * *

"In order to ensure that . . . an abdication of the magistrate's duty does not occur," the Supreme Court has instructed that courts must "conscientiously review the sufficiency of affidavits on which warrants are issued." *Gates*, 462 U.S. at 239. Here, for whatever reason – perhaps because the Bieniek Affidavit simultaneously sought to search five different accounts, blurring the lines between them and suggesting that the evidence with respect to each was more substantial than it was – Magistrate Judge Moses signed two warrants that were plainly not based upon probable cause. All of the evidence cited in the supporting affidavits was hopelessly stale. With respect to Mr. Archer and Mr. Momtazi's Google Accounts, probable cause was based on a *single* communication that was transmitted twenty-six months before the government applied for the Warrants. And not only did the Warrants authorize a search for and the seizure of categories of evidence for which the Bieniek Affidavit failed to provide probable cause, they also authorized a search for and the seizure of categories of evidence about which the Bieniek Affidavit was entirely silent, authorizing a wide-ranging fishing expedition. At a minimum, therefore, "the breadth of the search exceed[ed] the probable cause on which that search was based," meaning that "the government [has] run[] afoul of the Fourth Amendment," warranting suppression. *Feng Ling Liu*, 2014 WL 101672, at *7; *see also Tairod*, 2015 WL 9450598, at *19 ("The prohibition on overbreadth necessitates that the scope of the warrant be limited to the probable cause on which the warrant is based." (quotation omitted)); *Galpin*, 720 F.3d at 446 ("an otherwise unobjectionable description of the objects to be seized is defective if it is broader than can be justified by the probable cause upon which the warrant is based" (quotation omitted)).

III. THE WARRANT AFFIDAVIT CONTAINED INTENTIONALLY OR RECKLESSLY MISLEADING STATEMENTS

Although the Bieniek Affidavit itself fails to supply probable cause for the Warrants, it also omits certain critical information that, properly considered, further undermines any conceivable basis for the Warrants. In particular, the Bieniek Affidavit intentionally, or at least recklessly, failed to disclose (1) that Mr. Archer produced thousands of documents from the Archer Accounts, including all but one of the e-mails involving those accounts cited in the Affidavit;[21] and (2) that Jason Galanis was arrested on separate charges in September 2015 – long after all of the e-mails cited in the Affidavit had been sent. Taken separately, and especially together, these omissions further eroded any purported showing of probable cause in the Bieniek Affidavit. Had Magistrate Judge Moses known the full truth – especially given the scant evidence cited in the Bieniek Affidavit in the first place – there is no way that she would have issued the Warrants.

A. Relevant Facts

Other than one passing reference to conversations with "SEC staff attorneys about their review of [certain] records," Decl. Ex. 4 at 9, the Bieniek Affidavit does not disclose the substantial, nearly year-and-a-half-long SEC investigation that preceded the submission of the warrant application on December 28, 2016. *See id.* (referencing an FBI and USPIS investigation pending "[s]ince at least 2015" without mentioning the SEC investigation). According to a recent government filing in this case, the SEC's investigation began at least "in or around August 2015," Decl. Ex. 32 at 3, and as part of its investigation, the SEC came into possession of

[21] The one document cited in the Bieniek Affidavit that was not produced in response to a Grand Jury subpoena, the allegedly misleading "client representation letter" sent from the Momtazi Google Account, was actually *attached* to the Grand Jury subpoena to Mr. Archer.

millions of documents including, among many other things, "the entirety of [the] records" of the investment advisory firms at issue in this case. *Id.* at 4.

"[T]he Government submitted an access request letter to the SEC on or about January 20, 2016," which, once granted, "allowed the SEC to provide to the Government documents and materials that the SEC obtained as part of its investigation." *Id.* "Pursuant to that access request letter, the Government obtained millions of documents from the SEC." *Id.*[22] Moreover, as part of their coordinated investigations, the government and the SEC discussed their theories of liability with one another and "generally conducted witness interviews together," with representatives from both the U.S. Attorney's Office and the SEC typically asking questions, either an FBI or USPIS agent taking "the only notes and draft[ing] reports memorializing the interviews," and SEC attorneys occasionally travelling "to the U.S. Attorney's Office to review and create notes and/or memoranda from some, but not all, of those reports." *Id.* at 4. None of this was mentioned in the Bieniek Affidavit.

Most critically, the Bieniek Affidavit omitted the fact that, in the course of their coordinated investigations, Mr. Archer produced thousands of documents from the Archer Accounts to both the U.S. Attorney's Office and the SEC, long before the Bieniek Affidavit was sworn on December 28, 2016. Mr. Archer, for example, produced over 31,000 pages of documents to the U.S. Attorney's Office on May 9, 2016, *i.e.*, the very day that the government obtained its sealed complaint. Decl. ¶ 38. Of these, over 25,000 pages of documents came from the Archer Accounts. *Id.* Mr. Archer also produced nearly 9,000 pages of documents to the SEC

[22] The SEC has also purportedly "opened several investigations tangentially related to the Wakpamni matter." Decl. Ex. 32at 3 n.2. The government has represented that it "submitted access request letters to the SEC in connection with these matters on June 6, 2016 and November 14, 2016, respectively." *Id.* at 4. Neither of these purportedly "tangentially related" investigations were revealed in the Bieniek Affidavit, either.

on December 6 and 21, 2016, which Mr. Archer understands were provided to the U.S. Attorney's Office. *Id.* ¶ 39. As with the aforementioned production to the U.S. Attorney's Office, a great number of the documents in these productions to the SEC were taken from the Archer Accounts. *Id.*[23]

The government's failure to disclose that Mr. Archer had already produced tens of thousands of pages of documents from the Google and Apptix Accounts, and that the government therefore had received, as mentioned above, all but one of the e-mails cited in the Bieniek Affidavit, is inexcusable. The Bieniek Affidavit relied on only a handful of e-mails – a total of no more than thirteen – to support its purported probable cause showing, each one of which was, as explained above, well over two years old. Had the Magistrate Judge understood that Mr. Archer had already produced these e-mails, as well as thousands of others, the staleness concerns articulated above would have jumped out. Put differently, the government was required to supply probable cause to believe that fruits, instrumentalities, or evidence of the crime would still be contained in the Archer Accounts at the time of the search. The fact that Mr. Archer had turned over any conceivably relevant piece of evidence – and that the government was unable to find anything other than the handful of e-mails quoted in the Bieniek Affidavit, which Mr. Archer had himself produced – eviscerated the idea that the Archer Accounts would contain any other relevant evidence.

Separately, the Bieniek Affidavit also failed entirely to mention Jason Galanis's arrest on separate fraud charges in September 2015, stemming from his takeover of a company called Gerova and his manipulation of Gerova's stock. *See United States v. Galanis, et al.*, No. 15 Cr.

[23] Mr. Archer also understands that Bevan Cooney produced approximately 10,000 pages of documents, including many from the Cooney Account, in response to SEC and/or Grand Jury subpoenas, long before the issuance of the Warrants. The Bieniek Affidavit failed to disclose that fact, as well.

643 (PKC); *SEC v. Galanis, et al.*, 15 Civ. 7547 (VSB). As the Court is aware, Jason Galanis subsequently pleaded guilty to that fraud, but it is his arrest that was the critical omission from the Bieniek Affidavit, for reasons discussed below.

B. Legal Standard

In *Franks v. Delaware*, the Supreme Court held that a defendant is entitled, in certain circumstances, to a hearing to test the veracity of a warrant affiant's statements. *See* 438 U.S. 154, 171 (1978). "Where a defendant makes a preliminary showing that the government's [warrant] affidavit misstated or omitted material information, *Franks* instructs a district court to hold a hearing to determine" whether the alleged misstatements or omissions in the warrant application "were made intentionally or with reckless disregard" for the truth and, if so, whether any such misstatements or omissions were "material." *United States v. Rajaratnam*, No. 09-cr-1184 (RJH), 2010 WL 4867402, at *7-8 (S.D.N.Y. Nov. 24, 2010).

In other words, "[t]o suppress evidence obtained pursuant to an affidavit containing erroneous information, the defendant must show that: (1) the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the [issuing] judge's probable cause finding." *United States v. Canfield*, 212 F.3d 713, 717-18 (2d Cir. 2000) (internal quotation marks omitted and alteration in original); *see also United States v. Awadallah*, 349 F.3d 42, 64 (2d Cir. 2003) (noting that "[i]n order to invoke the *Franks* doctrine, [a defendant] must show that there were intentional and material misrepresentations or omissions in [the] warrant affidavit").

C. Special Agent Bieniek's Omissions Were Either Designed To Mislead Or Made In Reckless Disregard Of Whether They Would Mislead

There is no question that Special Agent Bieniek was well aware of the omitted facts when she swore out her affidavit, and that she nonetheless misleadingly omitted them. Special Agent Bieniek was personally involved in the underlying investigation, and had indeed attended meetings between Mr. Archer's counsel and the government (and SEC) in which Mr. Archer's counsel presented various documents he had previously produced, and generally appears to have been the case agent at or about the time that Mr. Archer made his productions. There is also no doubt that Special Agent Bieniek was fully familiar with the charges in the Gerova case. *See* Decl. ¶ 49. Among other things, she was part of the government's trial team in that case in or about September 2016, just months before she swore out the Bieniek Affidavit. *Id.* That being so, the omission of those facts from the Bieniek Affidavit was, at a minimum, reckless. *See, e.g.*, *United States v. Harding*, 273 F.Supp.2d 411, 426 (S.D.N.Y. 2003) ("[T]he preliminary issue to be resolved is whether Harding has shown that Agent Castro knew or had reason to know the 'facts' he omitted from the search warrant affidavit.").

Here, the affidavit makes only one passing reference to Special Agent Bieniek speaking with SEC staff attorneys. It makes no reference whatsoever to the facts that (1) the SEC had been investigating Mr. Archer and at least some of his co-defendants since August 2015; (2) the SEC had collected millions of documents as part of that investigation; (3) the SEC had provided millions of those documents to the U.S. Attorney's Office pursuant to its January 2016 access request letter; (4) the SEC and the U.S. Attorney's Office had conducted numerous joint interviews of witnesses as part of their coordinated investigations; (5) the SEC had opened up at least two purportedly tangentially related investigations, and presumably collected a substantial number of documents relating thereto, which the Government also requested, and presumably

received; and, most importantly, (6) Messrs. Archer and Cooney had already produced tens of thousands of pages of documents from the Targeted Accounts to both the U.S. Attorney's Office and the SEC, including all but one of the e-mails cited in the Bieniek Affidavit related to the Archer Accounts. Likewise, the Bieniek Affidavit fails to mention the Gerova fraud, generally, as well as, more specifically, Jason Galanis's 2015 arrest in that case.

And yet, Special Agent Bieniek elected to keep all of this information from Magistrate Judge Moses, deliberately giving her a woefully incomplete and entirely misleading portrait of the investigation that had been done, and therefore the likelihood that the Targeted Accounts would actually be a viable source of new evidence. *See, e.g.*, *Rajaratnam*, 2010 WL 4867402, at *9-10 (finding wiretap application "misleading" where it mentioned only an investigation ongoing since 2007 and "left out" the fact that a separate investigation had been ongoing since 1998).

Even if the aforementioned omissions do not evince a deliberate intention to mislead (which, on their faces, they do), the reckless disregard standard is nevertheless met here. Clearly, a magistrate judge being asked to take the extraordinary step of giving the government access to a citizen's private internet account would have wanted to know about the breadth of the SEC investigation and, perhaps most of all, whether that citizen had already voluntarily provided thousands of documents from that private e-mail account to both the government and the SEC. In light of the scant evidence connecting the Targeted Accounts to the crimes charged in the Indictment, the Magistrate Judge would have wanted to know that Messrs. Archer and Cooney had already produced thousands of pages of documents from those accounts, and that the slim pickings in the Bieniek Affidavit represented the best the government could do. Likewise, an issuing judge in Magistrate Judge Moses' position certainly would have wanted to know whether the e-mails being quoted in the warrant application were obtained by the government pursuant to

those voluntary productions by Messrs. Archer and Cooney, and she would have also wanted to know at least some of the details of those productions, including the fact that the productions contained thousands of documents, only a miniscule number of which were misleadingly quoted in the warrant application.

Likewise, the Magistrate Judge would have wanted to know that in the more than two years between the underlying events that supposedly constituted probable cause and the date of the warrant application, the alleged ringleader of the fraud had been arrested on separate charges – making it even less likely that other relevant e-mails would still be available if she issued the Warrants. This makes clear that the "omitted information was . . . critical to assessing the legality of the search," as the question of staleness goes directly to the question of the legality of the search. *United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir. 1996) (internal quotation marks omitted).

Accordingly, Mr. Archer has made a substantial preliminary showing that the many important facts that Special Agent Bieniek omitted from her affidavit were deliberately omitted, or were omitted with reckless disregard for the truth.[24]

D. The Omissions From The Bieniek Affidavit Were Material To The Magistrate Judge's Probable Cause Determination

For similar reasons, Special Agent Bieniek's omissions were clearly material to the Magistrate Judge's probable cause determination. Specifically, had the Magistrate Judge understood that the SEC had conducted a massive investigation and gathered millions of documents, *and* that Mr. Archer and Mr. Cooney had already produced responsive documents

[24] In addition, as set forth above, Special Agent Bieniek also made misleading statements about there being probable cause to believe that Mr. Archer had engaged in investment adviser fraud and conspiracy to commit investment adviser fraud, and that there was probable cause to support a search of the various aspects of his Google and Apptix accounts that went otherwise totally unaddressed in the affidavit.

from the Targeted Accounts, *and* that the Bieniek Affidavit reflected the best evidence the government could come up with having had the opportunity to review those thousands of documents, *and* that Jason Galanis – the central character in two different alleged frauds – had been arrested in between the time of the events supposedly giving rise to probable cause and the time of the warrant application, she would not have found probable cause. That is especially so in light of the meager evidence in the Bieniek Affidavit in the first place, such as the single e-mail that supposedly supplied probable cause for the entirety of the Archer and Momtazi Google Accounts.

To determine whether misstatements are "material," a court must "set[] aside the falsehoods" in the application, *United States v. Coreas*, 419 F.3d 151, 155 (2d Cir. 2005), and determine "[w]hether the untainted portions [of the application] suffice to support a probable cause finding," *United States v. Nanni*, 59 F.3d 1425, 1433 (2d Cir. 1995). Although omissions "are governed by the same rules" as misstatements, *United States v. Ferguson*, 758 F.2d 843, 848 (2d Cir. 1985), "the literal *Franks* approach [does not] seem[] adequate because, by their nature, omissions cannot be deleted"; therefore "[a] better approach . . . would be to . . . insert the omitted truths," *United States v. Ippolito*, 774 F.2d 1482, 1486 n.1 (9th Cir. 1985). Accordingly, the Second Circuit has held that "[t]he ultimate inquiry is whether, after putting aside erroneous information and [correcting] material omissions, there remains a residue of independent and lawful information sufficient to support [a finding of] probable cause." *Canfield*, 212 F.3d at 718 (internal quotation marks omitted); *see also United States v. Martin*, 615 F.2d 318, 328 (5th Cir. 1980) ("[W]e [are] required to determine whether, if the omitted material had been included in the affidavit, the affidavit would still establish probable cause. . . . If it would not, we would be required to void the warrant and suppress the evidence seized pursuant to it.").

The purpose of the Bieniek Affidavit was to attempt to demonstrate that the government needed access to the Targeted Accounts in order to obtain evidence, fruits, and instrumentalities of the crimes charged in the Indictment, and that there was substantial reason to believe that the Targeted Accounts would still contain any such evidence. Clearly, then, it would have been material to Magistrate Judge Moses' probable cause determination that Messrs. Cooney and Archer had *already* produced thousands of documents from the Targeted Accounts to both the government and the SEC. It would have also been material to the Magistrate's probable cause determination that, out of the thousands of documents produced by Mr. Archer, the government was only able to cherry-pick a small handful of such documents – each one innocuous on its face – to make its deeply flawed probable cause case against the two of them.

The omitted facts were also material because, as discussed above, the revelation of the SEC investigation, the breadth and extent of that investigation (and of the at least two supposedly tangentially related investigations), and the breadth of the prior document production by Messrs. Archer and Cooney would have emphasized the staleness of the facts purportedly giving rise to probable cause. *See supra*, Point II.A. Had Magistrate Judge Moses been apprised of these omitted facts, and the staleness of the facts upon which the government was relying in its warrant application, she would have found probable cause to be lacking, and would not have issued the Warrants.

The arrest of Jason Galanis in the Gerova case is also highly material for similar reasons. Had Magistrate Judge Moses understood that the admitted mastermind of the fraud was arrested a year after the e-mails supposedly given rise to probable cause were sent, the staleness of the evidence would have been even more apparent. That is, Jason Galanis's arrest in September 2016 made it far less likely that, in December 2016, e-mails from two years earlier evidencing communications with and about Galanis would still be in the Archer Accounts.

By way of analogy, a search of an alleged stash house based on information that someone had stored contraband there one time, more than two years earlier would be unconstitutional to begin with. But if the issuing magistrate also knew that the owner of the house had opened its doors to the police more than seven months earlier, *and* that she had told the police about that one instance when asked, *and* that the alleged leader of the conspiracy had been arrested three months earlier, there is no way a warrant for that house would issue. It is simply not plausible, on those facts, that there would still be any evidence in the house at that point, if there ever was.

* * *

Because Mr. Archer has made substantial preliminary showings that the many important facts that Special Agent Bieniek omitted from her search warrant affidavit were (1) deliberately omitted, or were omitted with reckless disregard for the truth, and (2) material to Magistrate Judge Moses' probable cause determination, this Court should suppress the fruits of the Warrants. At a minimum, the Court should hold a *Franks* hearing.

IV. THE WARRANTS WERE EXECUTED IN AN UNCONSTITUTIONAL MANNER

Putting aside the facial invalidity of the Warrants, the lack of probable cause underlying them, and the numerous material omissions from their supporting affidavit, the fruits of the Warrants should be suppressed for an additional, independent reason: The manner in which the government executed the Warrants exceeded their permissible scope so significantly that the Warrants were effectively (further) converted into constitutionally prohibited "general warrants."

A. Legal Standard

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against *unreasonable* searches and seizures." U.S. Const. amend. IV (emphasis supplied). The Fourth Amendment therefore "speak[s] to the manner of executing a warrant" insofar as "[s]uch execution is governed by the general touchstone of reasonableness

that applies to all Fourth Amendment analysis." *United States v. Ramirez*, 523 U.S. 65, 65-66 (1998) (citing *Pennsylvania v. Mimms*, 434 U.S. 106, 108-09 (1977); *see also King*, 563 U.S. at 459 ("The text of the Amendment thus expressly imposes [the] requirement[] . . . [that] all searches and seizures must be reasonable."); *see also Michigan v. Fisher*, 558 U.S. 45, 47 (2009) ("The ultimate touchstone of the Fourth Amendment, we have often said, is reasonableness." (quotation and alteration omitted)); *Wey*, 256 F. Supp. 3d at 380 ("In assessing the Constitutional sufficiency of any warrant, courts must be mindful that the ultimate touchstone of the Fourth Amendment is reasonableness." (quotation omitted)).

Thus, "a seizure lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution unreasonably infringes possessory interests protected by the Fourth Amendment's prohibition on unreasonable seizures." *United States v. Jacobsen*, 466 U.S. 109, 125 (1984) (quotation omitted). "[T]he reasonableness of a search is determined 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" *United States v. Knights*, 534 U.S. 112, 118-19 (2001) (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)).

Pursuant to the "blanket suppression doctrine," *Liu*, 239 F.3d at 140, "the suppression of *all* evidence seized is . . . justified [where] those executing the warrant acted 'in flagrant disregard' of [a] warrant's terms." *United States v. Matias*, 836 F.2d 744, 747 (2d Cir. 1988) (emphasis in original) (quoting *United States v. Medlin*, 798 F.2d 407, 411 (10th Cir. 1986)); *see also United States v. Medlin*, 842 F.2d 1194, 1199 (10th Cir. 1988) ("When law enforcement officers grossly exceed the scope of a search warrant in seizing property, the particularity requirement is undermined and a valid warrant is transformed into a general warrant thereby requiring suppression of all evidence seized under that warrant.")).

"The cornerstone of the blanket suppression doctrine is the enduring aversion of Anglo-American law to so-called general searches," and "[t]he rationale for blanket suppression is that a search that greatly exceeds the bounds of a warrant and is not conducted in good faith is essentially indistinguishable from a general search." *Liu*, 239 F.3d at 140-41 (citing, *inter alia*, *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 357 (1931) ("Since before the creation of our government, [general] searches have been deemed obnoxious to fundamental principles of liberty. They are denounced in the constitutions or statutes of every State in the Union. The need of protection against them is attested alike by history and present conditions." (alteration in original)). Thus, the Second Circuit has explicitly recognized that "wholesale suppression is required" when government agents "effect a widespread seizure of items that were not within the scope of the warrant, and . . . do not act in good faith." *Id.* at 140 (quotations omitted).

Here, the government has flagrantly disregarded the terms of the Warrants by effecting a widespread bad faith seizure of items outside of their scope in at least two distinct but interrelated ways.

B. The Government Has Knowingly Run Roughshod Over Mr. Archer's Attorney-Client Privilege, Seizing Privileged Documents That Do Not Fall Within The Scope Of The Warrants

First, the government has essentially ignored Mr. Archer's repeated protestations about the myriad problems inherent in using a wall AUSA to perform the privilege review that is still underway in this case, as set forth above. Instead, the government has insisted on undertaking a privilege review using methods that will inevitably disclose to it – and that have, in fact, disclosed to it – Mr. Archer's privileged information; refused numerous entreaties from Mr. Archer to undertake a more reasonable and prophylactic review; failed to provide almost any details about the particulars of its review protocol despite being asked repeatedly by Mr. Archer to do so; suggested that its wall AUSA may be tasked with deciding whether the so-called

"crime-fraud exception" applies to otherwise privileged documents; and baselessly rejected a number of plainly reasonable search terms that Mr. Archer asked it to use to screen for potentially privileged documents.[25] Taken collectively, all of these instances of the government's disregard for Mr. Archer's attorney-client privilege amount to a clear-cut case of bad faith, and assured that Mr. Archer's privilege would be trounced upon, with numerous privileged documents outside the scope of the Warrants being seized.

From the moment that Mr. Archer first learned about the warrants in January 2017, he has forcefully argued that the government's use of a wall AUSA or taint team would be woefully insufficient to protect all of the thousands of privileged communications strewn throughout the Archer Accounts. Mr. Archer has presented the government on multiple occasions with numerous cases, including several from within this District, that describe in detail why the privilege review still underway in this case is inherently problematic and completely inappropriate in criminal cases.

For example, because the government's privilege review procedure is premised on trusting the government to screen itself from information that it will naturally desire to see, courts have repeatedly called the procedure into question, both because of its failure to prevent the inadvertent disclosure of privileged information, *see In re Grand Jury Subpoenas*, 454 F.3d 511 (citing *United States v. Noriega*, 764 F. Supp. 1480 (S.D. Fla. 1991), wherein a taint team overlooked a document clearly protected by the attorney-client privilege), and because its very appearance is problematic, *see In re Search Warrant for Law Offices Executed on Mar. 19, 1992*, 153 F.R.D. 55, 59 (S.D.N.Y. 1994). As Judge Brieant explained:

[25] The government's review protocol was also substantially slower than the one proposed by Mr. Archer, to boot.

> [R]eliance on the implementation of a Chinese Wall, especially in the context of a criminal prosecution, is highly questionable, and should be discouraged. The appearance of Justice must be served, as well as the interests of Justice. It is a great leap of faith to expect that members of the general public would believe any such Chinese wall would be impenetrable; this notwithstanding our own trust in the honor of an AUSA. . . . Those on the Mongol side of the Wall may well access the same information from other sources, and have difficulty convincing a defendant or the public that the information did not pass over or through the Wall.

Id.

The inevitable problems that such privilege review methodologies present have led at least one circuit court to determine that a district court made reversible error in allowing the government to utilize a taint team to safeguard privilege. In *In re Grand Jury Subpoenas*, the Sixth Circuit considered the sole question of "whether the district court erred in preferring the government's proposed taint team to the appellants' own attorneys to make initial privilege determinations with respect to documents in the third-party subpoena recipient's possession." 454 F.3d at 516. The court determined that taint teams presented "inevitable, and reasonably foreseeable, risks," *id*. at 523; that historically they have "been implicated . . . in leaks of confidential information to prosecutors," *id*.; and that "human nature being what it is, occasionally some taint-team attorneys will make mistakes or violate their ethical obligations," *id*.*; see also United States v. Kaplan*, No. 02-cr-883 (DAB), 2003 WL 22880914, at *12 (S.D.N.Y. Dec. 5, 2003) ("Certainly this Opinion should be counted among those *disapproving* the Government's use of an ethical wall team to 'protect' the attorney-client and work-product privileges." (emphasis in original)).

Because the government has been deaf to his protestations and insisted on plowing ahead with its deeply problematic privilege review, Mr. Archer is now left at the mercy of a situation in which "the government's fox is left in charge of [his] henhouse," and will inevitably "err by

neglect or malice, as well as by honest differences of opinion," thereby vitiating his attorney-client privilege. *In re Grand Jury Subpoenas*, 454 F.3d at 523.

Additionally, and perhaps most egregiously, the government has suggested to counsel for Mr. Archer that the wall AUSA may be tasked with deciding whether the so-called "crime-fraud exception" applies to otherwise privileged documents. In response to this suggestion, Mr. Archer explained to the government that it would be profoundly inappropriate for the government to unilaterally determine that a document fell within the crime-fraud doctrine, or even for that determination to be made as part of the privilege review itself. Mr. Archer also apprised the government of *United States v. Levin*, No. 15-cr-101 (KBF), 2015 WL 5838579, at *2 (S.D.N.Y. Oct. 5, 2015), in which Judge Forrest was critical of a wall AUSA bringing a motion for a ruling that the crime-fraud exception applied to certain otherwise-privileged documents obtained via search warrant:

> The Court believes that the practice of having the Wall AUSA file a motion for application of the crime-fraud exception on behalf of the prosecution team conflicts with the Wall AUSA's intended role to prevent overbreadth of the Government's seizure of material pursuant to a search warrant. In the Wall AUSA's circumscribed role, he or she is not supposed to affirmatively act on behalf of the prosecution. Several courts in this district have expressed concern over the very practice of utilizing a Wall AUSA to conduct an initial review of seized material for potential privilege issues in the first instance. By bringing the instant motion, the Wall AUSA has gone one step further. What the Court finds particularly problematic in this instance is that the Wall AUSA, at least implicitly, bases her motion on her substantive awareness of the content of the documents at issue. This raises the potential Fourth Amendment concerns the ethical wall was intended to avoid.

2015 WL 5838579, at *2 (citations and footnotes omitted).

Nonetheless, a representative of the government's "taint team" has already identified to Mr. Archer a long list of documents that it claims may be subject to the crime-fraud exception. *See* Decl. Exs. 26 & 33. The government's approach here stands the purpose of a wall AUSA on

its head, and would allow the government to substantively benefit from the wall AUSA's having had access to the contents of privileged communications. *See Levin*, 2015 WL 5838579, at *2 ("As the wall is for the protection of the defendant's rights, it is decidedly not to give the Government a substantive look into that which it has no right to see."); *see also id.* at *2 n.5 ("[W]hen a Wall AUSA uses the very information seen to make a motion in the Court in which the criminal matter is being prosecuted, that Wall AUSA has stepped into substantive participation in the case.").

Moreover, despite stating before both this Court and the Second Circuit that it would work with Mr. Archer to devise a review protocol, *see* Decl. Ex. 9 at 16:25-17:8; Decl. Ex. 15 ¶ 41, the government:

- has refused, without any substantive discussion, to even consider Mr. Archer's proposed alternative review protocol modeled after the protocol adopted by the Sixth Circuit when faced with similar circumstances in *In re Grand Jury Subpoenas*;

- did not take Mr. Archer up on his willingness "to discuss having the Court employ a Special Master to run the [privilege segregation] search terms and separate the two batches of documents, if the government believes that is necessary";

- has never given Mr. Archer any indication of the way in which it is conducting its review, let alone informed him whether it would honor his requests that "anyone exposed to privileged material [during the privilege review would] be entirely isolated from the prosecution team," and not "seek guidance" from the prosecution team or its supervisors; and

- has not confirmed that it would document its privilege review protocol in writing, let alone shared that protocol with Mr. Archer.

Decl. Ex. 18 at 3-6 & n.3.

Instead, all the government did was permit Mr. Archer to send it a list of proposed search terms for isolating potentially privileged documents and communications. *See id.* at 8-9. Even then, however, the government rejected dozens of the search terms proposed by Mr. Archer

without any substantive discussion, agreeing only to run the proper names of individual lawyers and law firms identified by Mr. Archer. As a result, the government did not segregate for privilege review documents marked "Attorney Client Privileged," "Attorney Work Product," or the like – markings that typically designate potentially privileged communications, and which lawyers and their clients include precisely because they are so easily picked up on automated review.

The government's rejection of search terms provided by Mr. Archer in a good faith effort to protect his privileged communications was the nail in the coffin in ensuring that his privileged communications would evade the government's deeply problematic privilege review in the first instance and make their way directly to the prosecution team, to Mr. Archer's profound detriment, as even if such documents do not become trial exhibits, they will nevertheless inform the government's development of evidence, further investigation, or questioning at trial.

This is not a philosophical concern. As discussed above, Mr. Archer's review of the portion of the government's July 2017 production taken from the Archer Accounts – a production that supposedly had already removed documents identified as potentially privileged – revealed that the production included a number of privileged documents, including communications between Mr. Archer and the lawyers formerly representing him in this investigation about their defense strategy. *See* Decl. ¶ 30; *see generally United States v. Levy*, 577 F.2d 200, 210 (3d Cir. 1978) (reversing conviction and dismissing indictment where government obtained attorney-client information concerning defense strategy). To be clear, these were documents that, by the government's own admission, had been released to the prosecution team, *see* Decl. Ex. 23, at 2, and which necessarily tainted its investigation.

C. The Government Knowingly Seized, Retained, And Produced To All Of Mr. Archer's Co-Defendants Approximately 70,000 Documents That It Had Determined To Be Outside The Scope Of The Warrants

Second, and most astonishingly, the government has admitted that, in a gross violation of both his privacy and the Fourth Amendment, it not only seized and retained, but also *produced to all of Mr. Archer's co-defendants*, approximately 70,000 documents that it had explicitly determined to be non-responsive to the Warrants. *See generally supra*, "Relevant Background" Section F.

United States v. Metter, 860 F. Supp. 2d 205 (E.D.N.Y. 2012), is instructive on this point. In *Metter*, a multi-defendant conspiracy case like this one, Judge Irizarry granted blanket suppression of all electronic evidence seized pursuant to three different search warrants. *Id.* at 216. One of those three search warrants was for the defendant's personal e-mail account. Using that warrant, the government took "a snapshot of all of the activity that had occurred in [his] personal email account." *Id.* at 214. The government also imaged a number of computer hard drives pursuant to the other warrants. *See id.* at 210.

After fifteen months, during which time the parties litigated disputes highly reminiscent of those that have been litigated in this case about how the necessary privilege review would be conducted, *see id.* at 210, the government still "had not conducted its review of the evidence seized and imaged to determine whether any of that imaged evidence fell outside the scope of the search warrant[s]," *id.* at 211. Moreover, the government on one occasion "indicated that it intended to produce all of the imaged evidence (without reviewing it first) to all defendants," and on another occasion stated that it would either permit all defendants to inspect all of the imaged data at the government's offices or produce all such data to any defendant upon their provision of hard drives capable of storing it. *Id.* at 210-11.

The defendant's attorney objected to the government's proposed approaches on both occasions. On the first occasion, he took issue with the government's position that it could seize

> years' worth of confidential completely irrelevant material . . . and then disseminate it out to a group of other individuals. . . . This is really a matter of irrelevant personal confidential data. Heaven only knows what's on there. Financial data, personal information, relationship information. That cannot – that can't be permissible.

Id. On the second occasion, the defendant's attorney filed a letter indicating his continued objections to the notion that the government could seize a mass of electronic evidence, "fail to conduct any review of the extent to which the material far exceeds the scope of a warrant, but then disseminate that material to others." *Id.* at 211. Judge Irizarry noted, as well, that

> the seizure of a personal email account could, in addition to evidence responsive to a search warrant, yield personal communications between a cheating spouse and his or her paramour or communications between an individual and his or her family regarding an embarrassing medical condition. These hypothetical communications clearly fall outside the scope of the search warrants in this case (and arguably those in most criminal cases).

Id. at 212. Ultimately, however, the government did not actually make its threatened production of the contents of the defendant's full e-mail account or any of his hard drives to any of his co-defendants. *See id.* at 210-11.

Nonetheless, calling the government's "blatant disregard for its responsibility . . . unacceptable and unreasonable," Judge Irizarry proceeded to hold as follows:

> The government's retention of all imaged electronic documents, including personal emails, without any review whatsoever to determine not only their relevance to this case, but also to determine whether any recognized legal privileges attached to them, is unreasonable and disturbing. Moreover, the government repeatedly asserted its intent to release indiscriminately the imaged evidence to *every* defendant, prior to conducting any review to determine if it contained evidence outside the scope of the warrants. The Court agrees with Defendant that the release to the co-defendants of any and all seized electronic data without a

> predetermination of its privilege, nature or relevance to the charged criminal conduct only compounds the assault on his privacy concerns. It underscores the government's utter disregard for and relinquishment of its duty to insure that its warrants are executed properly.

Id. at 215 (emphasis in original). Applying the two-pronged "flagrant disregard" test, Judge Irizarry found that blanket suppression of all electronic evidence seized pursuant to the warrants was the appropriate remedy:

> The first prong is satisfied here as the "snapshot" the government sought permission to take resembles a general search. The warrants specifically sought, and the government was granted, permission for the widespread seizure of all information contained in the personal email accounts and computers at issue with imaging and review to occur off-site. The government subsequently "imaged" all of the seized items. There can be no doubt under these circumstances that this is a "general search" as described above.
>
> The lack of good faith by the government can be inferred from its conduct in this case. In the affidavits in support of the search warrants issued in this case, the government promised to review the evidence seized offsite to determine whether any evidence fell outside the scope of the warrants. The government then failed to commence the review, despite repeated requests from defense counsel and directions from the Court to do so. In fact, the government seemed shocked that the Court would require such a review, and, as mentioned above, threatened to provide *all* of the evidence seized and imaged to *each* defendant in the case, without conducting any such review. . . .
>
> The Court has not reached this conclusion lightly. However, the Court cannot, in the interest of justice and fairness, permit the government to ignore its obligations. Otherwise, the Fourth Amendment would lose all force and meaning in the digital era and citizens will have no recourse as to the unlawful seizure of information that falls outside the scope of a search warrant and its subsequent dissemination.

Id. at 215-16 (emphases in original).

Of course, in one sense, the government's conduct in this case is not as egregious as it was in *Metter*. Here, the government has at least commenced its responsiveness review, though

more than a year later the review remains ongoing, and it is still producing documents. *See* Decl. ¶ 42 & Ex. 23.[26] Specifically, the government claims to have used unknown "responsiveness" search terms to cull approximately 130,000 documents into two document sets: one containing approximately 70,000 documents that "were deemed non-responsive and will not be further reviewed," and another containing "approximately 58,000 potentially responsive emails" that "are being further reviewed for a final determination as to responsiveness." Decl. Ex. 23 at 2.

In another far more important sense, however, the government's conduct in this case has been vastly more egregious than it was in *Metter*. Rather than merely "assert[ing] its intent to release indiscriminately the imaged evidence to every defendant, prior to conducting any review to determine if it contained evidence outside the scope of the warrants" or "threaten[ing] to provide all of the evidence seized and imaged to each defendant in the case, without conducting any such review," *Metter*, 860 F. Supp. at 215-16 (emphases omitted), the government conducted a preliminary responsiveness review, determined that approximately 70,000 of the approximately 130,000 documents that it had seized were "non-responsive" and therefore outside the scope of the Warrants, *and then proceeded to produce all 70,000 of those documents to every defendant in this case anyway* – without any protective order in place, no less, leaving every one of Mr. Archer's co-defendants free to publicize literally *thousands* of his highly personal, sensitive, privileged, and/or confidential communications.

Moreover, given the fact that, as outlined above, certain of Mr. Archer's attorney-client, spousal, and other privileged communications evaded the government's so-called privilege review in the first instance and made their way directly to the prosecution team, Mr. Archer's

[26] Although the government's delay in this case is not as long as in *Metter*, it is significant that the Warrants in this case were issued post-Indictment, and that the government's review is ongoing with a looming trial date. In these circumstances, there is a more compelling need for the government to conduct its review promptly.

privileged communications were also included among the approximately 130,000 documents recklessly produced by the government. Accordingly, it is difficult to imagine a more grievous example of governmental bad faith in the execution of a search warrant for electronic information than that which the government has done here.

* * *

Thus, because the government has flagrantly disregarded the Warrants' terms by (1) failing to take the necessary measures to safeguard Mr. Archer's privilege in its review of the contents of the Archer Accounts, and (2) seizing, retaining, and producing to all of Mr. Archer's co-defendants without even a protective order in place *at least* approximately 70,000 documents that it had previously determined to be non-responsive[27] (and thus outside the scope of the Warrants if the Court finds that the Warrants actually have a "scope" and are not, as Mr. Archer believes, unconstitutional "general warrants" on their faces), including numerous privileged communications, it has "effected a widespread seizure of items that were not within the scope of the [W]arrant[s]" and acted in bad faith, such that "wholesale suppression [of the fruits of the Warrants] is required." *Liu*, 239 F.3d at 140.

V. THE GOOD FAITH EXCEPTION DOES NOT APPLY

This is not a case where the government can invoke the good faith exception to the exclusionary rule. *See generally United States v. Leon*, 468 U.S. 897 (1984).

To begin with, the good faith exception is not available when the government has made intentional or reckless misstatements in a warrant application, nor is it available when a warrant

[27] In addition to the 70,000 documents that the government deemed non-responsive based on the use of search terms, the government's subsequent review has apparently concluded that many of the remaining 58,000 documents were also non-responsive. Indeed, the government has thus far produced only approximately 10,000 documents from all of the Targeted Accounts that it claims to be responsive.

has been executed in an unconstitutional manner. *See id.* at 923 ("Suppression . . . remains an appropriate remedy if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth." (citation omitted)); *Raymonda*, 780 F.3d at 118 (finding that the good faith exception does not apply "in situations where an officer is 'reckless' or 'grossly negligent' in seeking or executing a warrant" (citing *Herring v. U.S.*, 555 U.S. 135, 144 (2009) ("[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct.")).

In addition, for the reasons given above, the government cannot invoke the good faith exception because no reasonable law enforcement officer could have thought that the Warrants were facially valid, or that the Bieniek Affidavit supplied probable cause to search the Targeted Accounts. *Raymonda*, 780 F.3d at 118 ("To claim the benefits of the good faith exception, . . . the officer's reliance on the duly issued warrant 'must be objectively reasonable.'" (quoting *Leon*, 468 U.S. at 922)); *id.* ("[T]he good faith exception cannot shield . . . an officer . . . where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable [or] where the warrant is so facially deficient that reliance upon it is unreasonable." (quoting *Clark*, 638 F.3d at 100)); *Cordova*, 792 F.3d at 1224 (holding that evidence of single transaction 22 months prior to search was so insufficient to establish probable cause officers could not even rely on warrant in good faith).

In this case, however, the good faith exception is not available for two additional reasons.

First, the government has affirmatively waived any reliance on the good faith exception. In volunteering that "the risk is on the government" when Mr. Archer tried to challenge the Warrants *before* they were executed, *see* Decl. Ex. 27 at 18:22; *see also id.* at 16:19 (AUSA stating: "Ultimately, the risk is on the government."), the government was explicitly acknowledging that it could not later claim good faith reliance on the fact that a Magistrate Judge

had issued the warrant. The Court's agreement that the "risk is on the government" acknowledged as much. *See generally Johnson v. Zerbst*, 304 U.S. 458, 464 (1938).

Second, even if the government had not explicitly waived reliance on the good faith doctrine, it would be inapplicable here because Mr. Archer put the government on explicit notice of the many problems with the Warrants and Bieniek Affidavit before it executed them. The rationale for the good faith rule is that the government should not have to suffer the exclusion of evidence – the purpose of which is to deter police misconduct, *see Utah v. Strieff*, 136 S. Ct. 2056, 2063 (2016) – if a neutral magistrate has signed a warrant, because the police are entitled to rely on the magistrate's determination, *see Leon*, 468 U.S. at 920-21. But here, the government was made aware of the problems with the Warrants and the Bieniek Affidavit and it nonetheless went ahead and conducted its search and seizure. In such a situation, the rationale of the good faith rule does not apply. *See Raymonda*, 780 F.3d at 119 ("Evidence obtained from a search should be suppressed only if the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional." (quoting *Leon*, 468 U.S. at 191) (alterations omitted)).

VI. THE GOVERNMENT SHOULD BE REQUIRED TO DISCLOSE ITS PRIVILEGE REVIEW PROTOCOL SO THAT MR. ARCHER CAN DETERMINE THE EXTENT OF ANY TAINT

As discussed above, with the exception of minimal correspondence on the topic of the search terms that Mr. Archer proposed to the government for the segregation of potentially privileged documents (most of which the government rejected out of hand), and a few high-level explanations of the basics of the privilege review process (mostly in court filings), the privilege review of the fruits of the Warrants by the government's so-called "wall AUSA" has taken place almost entirely behind the investigative curtain. Because Mr. Archer has been and remains in the

dark regarding the government's privilege review, he has asked the government to document the following in writing:

> a. The terms and methodology used to isolate potentially privileged documents from presumptively non-privileged ones[;]
>
> b. The review protocol as adopted, and the complete set of instructions and information given to the wall AUSA to follow in conducting his or her review, including the procedures for how and from whom to "seek guidance"[;]
>
> c. The contents and other particulars of any communications between the wall AUSA and anyone else on the subject of the review, including supervisors. . . . [; and]
>
> d. The manner in which the wall AUSA conducts his or her review, including his or her decision about which documents are privileged or non-privileged, and why.

Decl. Ex. 18 at 5. Unfortunately, the government has not provided Mr. Archer with any assurances that it has documented any of foregoing in writing, and to the extent that it has, in fact, documented any of the foregoing, Mr. Archer has not been given access to any such documentation.

Because the manner in which the government is conducting its secretive privilege review is vital to Mr. Archer's defense in this case, the Court should order an evidentiary hearing into all aspects of that review so that the Court and Mr. Archer can be satisfied that the government's case at trial (or members of the government's trial team) is not tainted by its invasion of his privilege. *See, e.g.*, Decl. Ex. 11 at 2 (denying Mr. Archer's motion for a stay pending appeal in part because any injury that Mr. Archer may suffer in the absence of his requested stay would not be irreparable given that, should he "determine at a later date that the Government has encountered privileged or other non-responsive materials, [he] can seek to suppress those materials, request a taint hearing, or even ask the Court to disqualify members of the Government team who encountered the materials").

VII. THE COURT SHOULD CONDUCT A TAINT HEARING

Because the Warrants are invalid, any e-mails and other evidence derived directly from the Warrants must be suppressed. But the Court should also conduct an evidentiary hearing to determine which other evidence should be suppressed as "fruit of the poisonous tree."

It is well-settled that, given an illegal search, evidence that "has been come at by exploitation of that illegality" is "taint[ed]" and must be excluded from use at trial. *Wong Sun v. United States*, 371 U.S. 471, 488 (1963). Given a "primary illegality," a defendant must be given some opportunity to resolve issues of taint. *Id.* at 488; *see also Nardone v. United States*, 308 U.S. 338, 341-42 (1939); *United States v. Vilar*, 530 F. Supp. 2d 616, 641 (S.D.N.Y. 2008) (it is clear that, once the defendant establishes that an illegal search has occurred, the Court "must" give some sort of "opportunity" for the defendant to satisfy his initial burden of showing taint in a "substantial portion" of the government's case; "there is no pre-hearing burden on the defendant to demonstrate taint in a substantial portion of the Government's case" (citations and quotations omitted)).

Evidence that derives, even indirectly, from an illegal search "must be suppressed unless the government proves, by a preponderance of evidence, that the evidence would have been discovered inevitably, was discovered through independent means, or that its discovery was so attenuated from the illegal search or seizure that the taint of the unlawful government conduct was dissipated." *United States v. Holmes*, 505 F.3d 1288, 1293 (D.C. Cir. 2007) (citing *Alderman v. United States*, 394 U.S. 165, 183 (1969) (noting that the government "has the ultimate burden of persuasion to show that its evidence is untainted")). While a hearing is not mandated, the Supreme Court has emphasized the value of an adversary proceeding in resolving such claims:

> Adversary proceedings will not magically eliminate all error, but they will substantially reduce its incidence by guarding against the possibility that the trial judge, through lack of time or unfamiliarity with the information contained in and suggested by the materials, will be unable to provide the scrutiny which the Fourth Amendment exclusionary rule demands.

Alderman, 384 U.S. at 184.

Here, Mr. Archer should be given the opportunity to participate in a full pre-trial taint hearing, in which he can seek to ascertain the full effect of the illegal search and seizure of the contents of the Targeted Accounts on the government's expected evidence at trial in this case, and to suppress any derivative evidence that the government obtained by exploiting that illegal search and seizure during its underlying investigation. At issue here is the government's exploitation of illegally-obtained evidence. Such serious misconduct should not be deferred until after a trial on the merits. *See, e.g.*, *United States v. McCall*, 489 F.2d 359, 363 (2d Cir. 1973) (disapproving of practice of postponing a taint hearing until after trial).

CONCLUSION

For the reasons just given, the Court should suppress any evidence obtained pursuant to the Warrants, directly or indirectly, and should order a hearing to determine the extent to which the government's subsequent evidence and investigation has been tainted by the search and seizure. Alternatively, the Court should conduct an evidentiary hearing on, among other things, the government's review protocols, as well as the misleading statements and omissions in the warrant affidavit.

Dated: January 22, 2018
New York, New York

Respectfully submitted,

/s/ Matthew L. Schwartz

Matthew L. Schwartz
BOIES SCHILLER FLEXNER LLP
575 Lexington Avenue, 7th Floor
New York, New York 10022
Tel.: (212) 446-2300
Fax: (212) 446-2350
mlschwartz@bsfllp.com

Attorney for Devon Archer